**Преступления в сфере высоких технологий. Предупреждение фактов мошенничества в социальных сетях.**

В последнее время на территории Гродненской области произошел рост количества фактов совершения одного из видов противоправных деяний в сети Интернет. 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.

Рассмотрим подробнее алгоритм противоправных действий преступника. Злоумышленник, используя небрежное отношение владельца сайта к обеспечению сохранности конфиденциальной информации (логинов, паролей) о пользователях либо беспечность самих пользователей, стремится получить реквизиты доступа к чужим учетным записям. При этом такая беспечность со стороны пользователей может проявляться в попадании на удочку «фишинговых» (имитирующих настоящий) сайтов; 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. На этом перечень способов завладения реквизитами отнюдь не исчерпан. Получив реквизиты, злоумышленник заходит в учетную запись жертвы, имеет возможность ознакомиться с ее содержимым, изучить список контактов, с которыми жертва поддерживает отношения. Зачастую преступник осуществляет смену пароля доступа к учетной записи, тем самым блокирует доступ законному владельцу к аккаунту. Далее злоумышленник осуществляет рассылку всем либо избранным контактам владельца взломанной учетной записи сообщения мошеннического характера.

Всё выше образует состав преступления таких статей Уголовного кодекса Республики Беларусь, как 349 «Несанкционированный доступ к компьютерной информации», 350 «Модификация компьютерной информации» и 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 Уголовного кодекса Республики Беларусь «Мошенничество». Когда имеет место предоставление потерпевшим платежных реквизитов и осуществление транзакций злоумышленником лично путем их ввода на различных сайтах, поддерживающих возможность совершения платежных операций, имеет место статья 212 «Хищение путем использования компьютерной техники».

Обратившись к статистике, можно констатировать: в текущем году на территории Гродненской области возбуждено порядка 50 уголовных дел по фактам несанкционированного доступа к учетным записям пользователей в сети Интернет, блокировки и модификации их содержимого. В результате зафиксировано более 30 случаев хищения денежных средств граждан, при этом наблюдается паритет мошенничеств и хищений путем использования компьютерной техники.

**Рекомендации как не попасть на удочку злоумышленников и обезопасить себя**:

− 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);

− 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;

− 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, 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), 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.

К сожалению, дать рекомендации о поведении в каждом возможном случае невозможно, но в общем случае, можно предложить пользователям в любой ситуации не терять бдительность и критическое отношение к окружающим нас явлениям и событиям.

Ст. оперуполномоченный ГРПСВТ КМ

ОВД Лидского райисполкома

ст. лейтенант милиции М.П. Пасюта