Состояние дел в области компьютерных преступлений в Новополоцке
и меры их предотвращения

Ввиду стремительного проникновения информационных технологий во все сферы жизнедеятельности человека, а также наряду с не высокой квалифицированностью определенной части граждан, в Республике Беларусь наблюдается устойчивая тенденция роста преступлений по направлению деятельности органов внутренних дел в сфере высоких технологий. Большая часть таких преступлений, выражающихся во «взломе» и несанкционированном использовании учетных записей пользователей в социальных сетях, и последующем хищений средств с банковских счетов пользователей путем мошенничества либо использования компьютерной техники.

Общее количество выявленных преступлений по линии СВТ за указанный промежуток времени составило -71 (2018 – 28) из них по 33 установлены подозреваемые лица (2018 - 18).

По видам преступлений:

- по ст.212 УК Республики Беларусь (хищения с использованием компьютерной техники) совершено – 58 /30 раскрыто (2018 – 24 /16 раскрыто), раскрываемость 51,7% (2018 –66,7%);

- по ст. 349 УК Республики Беларусь (несанкционированный доступ к компьютерной информации) – 11 /1 раскрыто (2018 – 3/2 раскрыто), раскрываемость 9,1% (2018 – 66,7%);

- по ст. 350 УК Республики Беларусь (компьютерный саботаж) -1 /1 раскрыто (2018 – 0 /0 раскрыто), раскрываемость 100%;

- по ст. 352 УК Республики Беларусь (неправомерное завлвдение компьютерной информацией) -1 /1 раскрыто (2018 – 0 /0 раскрыто), раскрываемость 100%;

В структуре преступлений по направлению деятельности СВТ, преобладают деяния, квалифицированные по ст.212 УК, в ходе изучения уголовных дел указанной категории установлено, что более половины, совершенных преступлений были осуществлены посредством несанкционированного доступа к учетным записям пользователей в социальной сети «В контакте» и «Одноклассники», где в последующем неустановленный преступник, выдавая себя за законного владельца «взломанной» страницы, обманом завладевал реквизитами банковских карточек потерпевших и похитил с них деньги путем интернет платежей;

Преступники осуществляют несанкционированный доступ к учетным записям в социальных сетях, сервисах электронной почты, аккаунтам в различных программах для обмена сообщениями, пользуясь небрежным отношением законного пользователя, выражающимся в:

* «воде логинов и паролей своих учетных записей соц. сети или электронных почтовых ящиков на иных, не имеющих отношения к функционированию указанных сервисов, сайтах:
* использовании одинаковых логинов и паролей на различных ресурсах:
* использовании слишком легких паролей:
* отсутствии на устройствах средств, позволяющих блокировать работу вредоносных программ:
* передачи третьим лицам банковских реквизитов либо реквизитов доступа к компьютерной информации.

Получив доступ к учетной записи жертвы, преступник осуществляет рассылку контактам владельца взломанной учетной записи сообщения мошеннического характера, варианты формулировок которых многочисленны, хитры и разнообразны, приведём лишь некоторые примеры таких сообщений:

* «Я нахожусь в России, у меня украли кошелек и телефон. Срочно вышли деньги на билет домой. Отправь мне на карт-счет (здесь может быть мобильный номер телефона, кошелёк в электронных платежных системах Яндекс. Деньги. QIWI, Web Money или других) 100 рублей. Все верну по приезду»;
* «У тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, па нее придут деньги, потом отдашь мне. В долгу не останусь!»

Для снижения вероятности совершения в отношении Вас данных преступлений важно соблюдать определенные рекомендации и правила при работе в сети Интернет:

* для выхода в сеть Интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;
* при использовании неизвестных Вам сайтов, обращайте внимание на их адрес в сети Интернет: возможно Вы зашли на поддельную его копию;
* 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;
* при поступлении сообщений от знакомых или сотрудников банка, 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;
* 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.

В случае если Вам стало что-либо известно о лицах или фактах совершения на территории г.Новополоцка преступлений в сфере высоких технологий сообщите об этом в подразделение Новополоцкого ГОВД по тел. 8 0214 50-70-13.

Старший оперуполномоченный ГРПСВТ

КМ Новополоцкого ГОВД

капитан милиции Д.Н. Свяцкий