ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫМИ С ХИЩЕНИЯМИ И МОШЕННИЧЕСТВОМ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ.

Государство и общество находятся в постоянном и непрерывном процессе развития. В таком же непрерывном процессе совершенство­вания и преобразования находятся информационные технологии. И ес­ли ранее момент появления и распространения их в обществе ассоции­ровался с безусловным прогрессом, новациями, шагом вперед, то позд­нее, когда в этой сфере стали совершаться противоправные деяния, в отношении законопослушных граждан, положительное отношение к информационным технологиям и самому процессу информатизации общества перестало быть столь непреклонным и неизменчивым.

Следует отметить, что к преступлениям в области информацион­ных технологий относятся не только преступления, предусмотренные гл. 31 Уголовного кодекса Республики Беларусь «Преступ­ления против информационной безопасности», но и противоправные деяния, предусмотренные иными статьями и главами УК. К числу преступлений в данной сфере относится и хищение с использованием компьютерной техники (cт. 212 УК), где компьютерная техника используется именно в качестве орудия со­вершения преступления.

В рамках своей деятельности Отдел «К» также значительное внимание уделяет вопросу предупреждения преступлений в сфере информаци­онных технологий, путем осведомления граждан всевозможными спо­собами о правилах безопасного пользования сетью Интернет, банков­скими платежными картами, о зарегистрированных фактах преступ­ного воздействия на информационную безопасность граждан для уменьшения количества жертв подобных преступлений. Деятельность такого характера ведется как в сети Интернет – на официальном сайте МВД Республики Беларусь, так и по телевидению, в газетах.

Однако, для предотвращения преступлений в IT-сфере, нельзя за­бывать и о роли самих пользователей информационными технология­ми, которые могут, соблюдая некоторые правила рекомендации, не стать жертвами подобных преступлений, а значит, непременно снизят количество преступных деяний в данной сфере.

К таким правилам следует отнести:

1. Не следует соглашаться покупать SIM-карты на свои паспорт­ные данные для малознакомых людей;
2. Нельзя предоставлять неизвестным конфиденциальные сведе­ния, размещенные на Вашей SIM-карте;
3. Не переходите по ссылкам, указанным в СМС - сообщениях, преходящих на Ваш мобильный телефон от незнакомого абонента; не скачивайте картинки, содержащиеся такого рода сообщениях;
4. Знайте, что органы МВД не уведомляют посредством сети Ин­тернет или мобильной связи о необходимости уплаты электронных штрафов;
5. Знайте об опасностях загрузки из сети Интернет различных программных продуктов! Внимательно читайте онлайновые объявле­ния! Не нажимайте «ок», если точно не знаете, с чем вы соглашаетесь;
6. Не общайтесь в социальных сетях, посредством электронной почты с незнакомыми Вам людьми, так как в последнее время все ча­ще именно такой способ используется для вербовки в террористиче­ские организации;
7. Не указывайте открыто свой e-mail адрес при размещении сво­их сообщений комментариев к статьям и т.д. на различных Интернет- форумах, в гостевых книгах и чатах.
8. Никогда не открывайте письма, поступившие от неизвестного отправителя, тем более прикрепленные файлы, которые могут содер­жать вредоносные программы.
9. Ни при каких условиях не следует отвечать на письма (другие со­общения и послания) сомнительного содержания от неизвестных пользо­вателей, показывая тем самым, что ваш e-mail реально существует.
10. Перед тем, как снять деньги посредством использования бан­комата, убедитесь в отсутствии установленного на него «скимера». Злоумышленники взламывают компьютерные системы банков, откуда воруют информацию о реквизитах банковских карт клиентов или при помощи специальной накладки («скимера») на клавиатуру банкомата, снимают данные с магнитных полос карточек. Похищенные сведения записывают при помощи специального устройства на фальшивые кре­дитки. С помощью такой подделки в банкомате снимают деньги или заказывают дорогостоящие товары в Интернет-магазинах;
11. Также, перед тем, как снять деньги посредством использова­ния банкомата, убедитесь в отсутствии на клавиатуре самого банкома­та металлической накладки, посредством которой преступники имеют реальную возможность узнать пароль от карты;
12. Опять же, перед тем, как снять деньги посредством исполь­зования банкомата, убедитесь в отсутствии «ливанской петли». Ис­пользуя специальное устройство («ливанская петля» — капроновая нить с металлической скобой), злоумышленники блокируют карточку в картприемнике банкомата. При возникновении затруднений с воз­вратом карточки, стоящий сзади человек предлагает пострадавшему повторно набрать ПИН-код. Благодарный гражданин теряет бдитель­ность и, не таясь, набирает код повторно. Конечно, банковская карта не воз­вращается и рассерженный клиент отправляется в банк, в то время как «добровольный советчик» извлекает карточку и снимает деньги.
13. Получив подозрительное сообщение, ни при каких обстоя­тельствах не вводите логин и пароль интернет-банка. Подобные махи­нации («фишинг») направлены на хищение паролей и персональных данных пользователей интернет-банков. Фишер (от англ. «fish» - ры­ба) - категория виртуальных мошенников, которая создает в сети Ин­тернет копии сайтов, например, банковского учреждения. После этого начинается «рыбалка». Рассылаются рекламные сообщения с завлекаю­щим текстом, на которые некоторые пользователи клюют, заходят на сайты-ловушки и оставляют там свои реквизиты (ПИН-код, номер счета). В скором времени банковские счета доверчивых людей пустеют.

Безусловно, нельзя говорить о полном искоренении преступности в сфере информационных технологий, так как с развитием самих тех­нологий, развиваются преступники, и способы совершения преступ­ления, и технические средства для совершения преступлений. Однако, можно с уверенностью утверждать, что своевременная профилактика таких преступлений Отделом по раскрытию преступлений в сфе­ре высоких технологий, а также бдительность самих граждан снизит уровень преступности в сфере информационных технологий.