Преступления в сфере высоких технологий

В 2020 года на территории Щучинского района зарегистрировано 66 преступлений в сфере высоких технологий, что на 48 преступлений больше чем в 2019 году, Данный вид преступлений выражается 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 использования компьютерной техники, либо мошенничества. И в обоих случаях злоумышленники пользуются излишней доверчивостью и неосмотрительностью самих пользователей, а также их халатным подходом к обеспечению безопасного использования сети Интернет и некоторым несовершенством банковских инструментов.

Учитывая изложенные выше факты, приведем некоторые рекомендации для пользователей сети интернет, которые могут снизить вероятность совершения в отношении них противоправных деяний:

– для выхода в сеть интернет используйте устройства, на которых установлено специальное программное обеспечение, предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;

– используйте операционную систему с установленными обновлениями безопасности, актуальные версии другого программного обеспечения, скачанные из официальных магазинов приложений;

– при использовании известных Вам сайтов, обращайте внимание на их внешний вид и адрес: 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 на зеленом фоне);

– 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.), периодически изменяйте свои пароли;

– по возможности используйте двухфакторную аутентификацию, когда кроме ввода логина и пароля необходимо вводить временный код, отправляемый обычно на мобильный телефон в виде SMS-сообщения либо push-уведомления;

– 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 (финансовые учреждения почти никогда не запрашивают финансовую информацию по электронной почте), 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, мессенджер, поддерживающий голосовую связь), либо в крайнем случае идентифицируйте личность собеседника путем задачи контрольных вопросов, ответы на которые не могут быть известны третьим лицам;

– не храните реквизиты карты в открытом доступе, в том числе в виде фотографий, не передавайте карту третьим лицам;

– если Вы не используете банковскую платежную карточку для осуществления интернет-платежей, обратитесь в банк для установки соответствующих ограничений для карты;

– используйте для платежей в сети интернет специализированные карточные продукты с отдельным счетом, обязательно подключите SMS-информирование о совершении расходных транзакций;

– 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 получения информации о несанкционированном списании средств с карточки незамедлительно принимайте меры к ее блокировке путем обращения в службу поддержки банка по телефону либо через интернет-банкинг, а также обращайтесь в банк с целью инициирования процедуры опротестования мошеннических транзакций, а также рассмотрения возможности возврата денежных средств в соответствии с принципом нулевой ответственности.

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но в общем можно предложить пользователям в любой ситуации не терять бдительность и критическое отношение к происходящему в сети интернет.

В законодательстве Республики Беларусь предусмотрена ответственность, в том числе уголовная за совершение противоправных деяний в сфере высоких технологий.

В случае совершения в отношении Вас противоправных деяний, рекомендуем Вам в кратчайшие сроки обратиться в органы внутренних дел по месту жительства либо обнаружения факта совершения преступления.

Ваша бдительность убережет Вас и Ваших знакомых от противоправных посягательств со стороны третьих лиц!