

Информация для проведения профилактических выступлений по направлению деятельности в сфере высоких технологий.

Анализируя оперативную обстановку по направлению деятельности в сфере высоких технологий, можно отметить, что с каждым годом наблюдается рост преступлений в данной сфере. В 2018 году преступлений по линии СВТ было 393. В 2019 году – 1177 преступлений, что в 3 раза больше показателя 2018 года.

Рост количества зарегистрированных преступлений рассматриваемой категории характерен для республики в целом, где он превысил более чем двух кратный показатель прошлого года.

В то же время рост преступности в сфере высоких технологий обусловлен следующими, конкретными факторами:

- расширением за последние годы сфер применения мобильных технологий при проведении безналичных платежей;
- значительным ростом количества пользователей глобальной сети Интернет;
- информационно-правовой неграмотностью населения в сфере высоких технологий.

Наиболее влияющим на сложившуюся обстановку является последний из обозначенных факторов связанный с финансовой и компьютерной неграмотностью населения, а также халатным отношением последних к сведениям о логинах и паролях от своих учетных записей зарегистрированных в сети Интернет и сведениях (составляющих банковскую тайну) о личных банковских счетах.

К сожалению, уровень компьютерной грамотности противоправных элементов постоянно совершенствуется, постоянно реализуются новые схемы совершения преступлений в сфере высоких технологий.

Анализируя изменения в преступных схемах, используемых на территории региона можно отметить, что в настоящее время наиболее актуальны противоправные действия, направленные на завладение платежными реквизитами банковских счетов граждан реализуемые на методах социальной инженерии и психологического воздействия на потерпевших с использованием телефонных вызовов.

В данных схемах злоумышленники звонят на абонентские номера операторов мобильной связи потерпевших и от имени сотрудников банков выведывают у последних информацию необходимую для получения доступа к банковскому счету и возможности распоряжаться находящимися на счету денежными средствами.

Потерпевшего подкупает то, что злоумышленники обращаются к потерпевшему по имени отчеству и в ряде случаев достоверно знают клиентом какого банка он является, и даже в единичных случаях

приблизительный баланс денег на счете. Все рассматриваемые сведения о данных гражданах, как правило, злоумышленники получают путем детального анализа его социальных сетей. Ввиду чего, следует очень внимательно относиться к информации, размещаемой о себе в сети Интернет.

Основным обстоятельством, способствующим получению от потерпевшего необходимых сведений является предрасположенность последнего к психологическому воздействию и личная доверчивость. В случаях когда человек не идет на контакт с злоумышленниками и подвергает сомнению все его доводы завладеть конфиденциальной информацией о счете не удается.

Дабы не стать жертвой киберпреступлений настоятельно рекомендую не сообщать никому в телефонном режиме свои паспортные и иные личные данные, реквизиты счетов банковских платежных карт, а также содержание СМС-сообщений поступающих с банковских учреждений. В случае поступления подобных звонков рекомендую незамедлительно окончить разговор и оставлять без ответа аналогичные входящие вызовы.

Помните! Сотрудники банковских учреждений не вправе по собственной инициативе выяснять у клиента в телефонном режиме указанные сведения!

Разглашение указанных сведений третьим лицам является основанием для отказа банком в возврате похищенных денежных средств!

В случае если все же указанная ситуация случилась и деньги со счета пропали, незамедлительно обращаться в банк, сразу по телефону указанному на сайте банка либо на банковской карте и далее, в обязательном порядке с письменным заявлением в банк.

Помните, только письменное заявление в банк является основанием для возможного возврата денежных средств по оспариваемым операциям.

Решение о возврате денежных средств принимается только сотрудниками банковского учреждения счет в котором скомпрометирован. Данное решение, в том числе зависит от результатов проверок проводимых ОВД.

Анализируя рассматриваемые преступления по потерпевшим, можно отметить, что большинство из них в возрасте от 30 до 45 лет со средним достатком, 70 % - женщины, из которых практически все имеют высшее образование, в том числе среди них имеются сотрудницы банковских учреждений, и крупных IT-компаний.

Не смотря на то, что злоумышленники действуют с высокой степенью сокрытия следов в сети Интернет и владеют программным

обеспечением, позволяющим оставаться анонимным в сети Интернет, на территории республики уже задержаны ряд организованных групп занимавшихся преступлениями по подобной схеме, которым в соответствии с действующим законодательством грозит от 5 до 12 лет лишения свободы. Имеются наработки и в нашем отделе.

Обращаясь к нашим абонентам, хочу напомнить о неотвратимости наказания и уверить, что даже год лишения свободы не стоит никаких денег, а 12 лет тем более!