МАТЕРИАЛЫ

для членов информационно-пропагандистских групп

(январь 2020 г.)

**ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ**

**(СТАТЬЯ 212 УГОЛОВНОГО КОДЕКСА РЕСПУБЛИКИ БЕЛАРУСЬ)**

Статистические сведения о состоянии преступности в Республике Беларусь свидетельствуют об устойчивой динамике роста количества совершаемых преступлений в сфере высоких технологий. Так за 10 месяцев 2018 года на территории Республики Беларусь зарегистрировано 2387 преступлений по статье 212 Уголовного кодекса Республики Беларусь (хищение путём использования компьютерной техники), то за аналогичный период этого года количество таких преступлений увеличилось более чем в два раза – 4863 (+103,7%).

Анализируя оперативную обстановку по направлению деятельности в сфере высоких технологий, по состоянию на десять месяцев 2019 года, в Речицком районе количество зарегистрированных хищений с использованием компьютерной техники (ст. 212 УК РБ) составляло 52 преступления, из них установлены подозреваемые лица по 21 уголовному делу. За аналогичный период прошлого года, данный показатель составил 13 преступлений, из них установлены подозреваемые лица по 5 уголовным делам. По преступлениям в сфере информационной безопасности (ст.ст. 349-355 УК РБ) количество зарегистрированных преступлений за выше указанный период времени 2019 года, составило 19 преступлений (АППГ 4).

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.

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 и 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 относится 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.

*Например, в ноябре текущего года жительница г. Гомеля лишилась денежных средств в размере 2500 долларов США и 16870 рублей следующим способом. На мобильный телефон последней позвонил неизвестный мужчина, который представился сотрудником банка и поинтересовался, подтверждает ли она заявку на кредит, которую она направила 30 минут назад. Женщина ответила отрицательно. Далее от мужчины последовал ряд вопросов, в том числе об утере банковской карточки или паспорта. Затем он сообщил, что в заявке на кредит от её имени указано, что женщина обладает банковской картой другого банка. После того как потерпевшая сообщила злоумышленнику название банка, он якобы переключил её на телефонную линию этого банка.*

*Затем последовал длительный разговор с «сотрудником службы безопасности» банка, клиенткой которого является потерпевшая. Мужчина убедил, якобы для предотвращения мошеннических действий, сообщить реквизиты одной из её банковских карточек, паспортные данные, содержание нескольких СМС с кодами для подтверждения операций. Злоумышленник предупредил женщину, что в целях безопасности её деньги временно будут переведены на «сейфовую ячейку» банка с блокировкой расчётного счёта и доступа к личному кабинету в интернет-банкинге.*

Дабы не стать жертвой киберпреступлений настоятельно рекомендуется 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 рекомендуется незамедлительно окончить разговор и оставить 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 произошла и деньги со счета пропали, незамедлительно позвоните по телефону указанному на сайте банка либо на банковской карте и заблокируйте счет. После чего в обязательном порядке обратитесь в банк с письменным заявлением и получите выписку по счету. Затем с выпиской по счету и копией обращения в банк обратитесь в правоохранительные органы по месту жительства.

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 IТ-компаний.

Несмотря 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.

Почти каждое пятое преступление, предусмотренное ст. 212 УК совершено с использованием мобильных телефонов потерпевших посредством установки программного приложения «А1-banking», при помощи которого злоумышленники получали кредит в размере до 100 рублей и распоряжались им по своему усмотрению.

Злоумышленники под различными предлогами, например, для срочного звонка или необходимости зайти в социальную сеть, просят граждан воспользоваться их мобильными телефонами, после чего в течение нескольких минут устанавливают программное приложение и получают «мобильный» кредит. После этого быстро переводят деньги на свой расчётный счёт, электронный кошелёк или другой абонентский номер.

**Уберечь себя от подобного вида воровства** поможет несложное правило: старайтесь никому не давать позвонить со своего телефона. Универсальная отговорка: отключены исходящие звонки. Если отказать в помощи вы не можете (к вам обратился человек, находящийся в отчаянном состоянии или подросток), то совершите звонок самостоятельно, не давайте посторонним людям свой телефон.

Ещё одним способом совершения подобных преступлений является рассылка сообщений в социальных сетях, мессенджерах, форумах якобы от имени друзей или даже администрации сайта.

*В сообщениях указано, что один из банков в связи с юбилеем или другим праздником дарит своим клиентам «денежные» подарки для чего требуется сообщить данные банковской карты или оплатить комиссионный сбор для «открытия счёта». Результатом сообщения своих персональных данных является списание всех денежных средств с карт-счетов доверчивых клиентов, а все «комиссионные сборы» просто оседают в карманах мошенников.*

**В подобных случаях** настоятельно **не рекомендуется** переходить по ссылкам (даже для того, чтобы «просто посмотреть»), а уж тем более — переводить деньги.