Тезисы выступления перед населением по вопросу *«Профилактика хищений, совершенных посредством использованием информационно-телекоммуникационных технологий»*

Уважаемые граждане!

Анализ оперативной обстановки на территории республики свидетельствует о значительном переходе преступного элемента в киберпространство для совершения посягательств на имущество граждан. Количество традиционных составов преступлений, таких как кражи, грабежи, мошенничества при непосредственном контакте потерпевшего и преступника неуклонно снижаются, при этом число хищений с использованием информационно-телекоммуникационных технологий растет. Данная проблема представляет угрозу национальной безопасности.

По итогам 8 месяцев 2024 года в республике зарегистрировано более 9 тысяч хищений, совершенных с использованием информационно-телекоммуникационных технологий *(мошенничества общеуголовной направленности – 6758, кражи с банковских карт - 2373)*.

Суммарный ущерб хищений с использованием IT-преступлений по состоянию на 8 сентября 2024 года составил более 2,6 миллиардов рублей – и это, подчеркиваю, только в отношении жителей нашей республики!!!

Необходимо отметить, что пострадавшими от преступлений с использованием IT-технологий являются различные категории граждан, при этом в большинстве случаев, люди с невысокими доходами, работники бюджетной сферы, пенсионеры, незащищенные слои граждан, которые имеют низкие знания финансовых

инструментов и последствий от совершения определенных действий, в том числе в сфере дистанционного банковского обслуживания.

*****

Основная доля *(около 75%)* в общем количестве преступлений, с использованием информационно-телекоммуникационных технологий совершается с использованием преимущественно двух способов – социальной инженерии по каналам мобильной или интернет связи и при покупке-продаже различных товаров.

Наибольшую проблему для раскрытия представляют преступления, совершенные методами социальной инженерии под видом сотрудников банков *(около 30% от общего числа мошенничеств и краж с карт)*, когда злоумышленники с использованием Интернет-телефонии, имитируя работу колл-центра банковского учреждения и используя терминологию сотрудников банков, вводят в заблуждение о якобы несанкционированном списании денег с банковской карты или оформлении кредитов; затем предлагают перевести деньги на «безопасный» счет преступников, либо сообщить реквизиты банковской карты и коды подтверждения банковских операций. В последнее время мошенники представляются должностными лицами полиции, ФСБ и прокуратуры, работающими как будто в связке с работниками банков. Вводя в заблуждение своих жертв в оказании помощи в поимке преступников, либо угрожая уголовной ответственностью о якобы совершенных переводах со счетов потерпевших за пределы Российской Федерации, они убеждают граждан переводить свои сбережения, а нередко и заемные средства, на якобы безопасные счета, которые фактически похищаются.

Вот, например, стандартная ситуация. В Отдел полиции №7 обратился главный специалист Территориального органа Федеральной службы по надзору в сфере здравоохранения по республике о том, что неизвестные, позвонив на сотовый телефон представившись сотрудниками ФСБ и Центрального Банка похитили денежные средства в сумме 1 миллион рублей, которые она взяла в кредит и перевела через банкоматы на неустановленные счета. Более того, она дальше пошла брать кредит в сумме 1 миллион рублей в другом банке, чтобы перевести мошенникам, но настоящие работники банка поняв, что потерпевшая находится под чужим воздействием вызвали сотрудников полиции и тем самым предотвратили отправку еще одного миллиона мошенникам.

В Отдел полиции №6 обратился 65-ти летний пенсионер, который по аналогичной схеме через банкоматы г.Уфы перевел мошенникам 5 млн. 852 тыс. рублей (личные накопления и кредитные средства). Со слов потерпевшего в торговых центрах возле банкоматов во время внесения денежных средств к нему подходили сотрудники полиции, которые проводили с ним профилактическую беседу, но он не придал этому значения.

*****

Еще один убедительный предлог мошенничества, который начал использоваться с конца прошлого года – это случаи, когда мошенник звонит и, представляясь сотрудником сервиса «Госуслуг» либо Многофункционального центра, просит Вас получить заказное письмо, но для этого необходимо назвать код подтверждения из СМС-сообщения. На самом деле СМС с кодом приходит Вам не для

получения письма, а для доступа либо к Вашему личному кабинету на сервисе «Госуслуги», либо к личному кабинету Мобильного банка. Вы понимаете, что, допустив мошенника к любому своему личному кабинету, Вы в считанные минуты можете стать без Вашего же ведома обладателем большого потребительского кредита, который опять же без Вашего ведома уйдет на сторонние счета.

Характерная фабула:

Начальнику диспетчерской службы крупной нефтесервисной компании в приложении «WhatsApp» поступил звонок с ранее незнакомого номера, фото профиля логотип «Госуслуги», звонил мужчина, представился сотрудником «Госуслуги» и сообщил, что с МФЦ должен поступить файл, для того чтобы его получить поступит смс-сообщение с кодом подтверждения, который потерпевший должен сообщить. Затем этому гражданину поступило смс-сообщение с кодом подтверждения, который он сообщил звонящему мужчине. Через несколько минут поступил звонок с другого номера, звонила женщина представилась сотрудником «Госуслуг», сообщила, что аккаунт на сайте «Госуслуги» пытаются взломать, спросила говорил ли он кому либо код подтверждения из смс-сообщения, потерпевший сказал, что сообщал, на что девушка поругала его и сказала, что звонили мошенники и что нельзя было говорить им код из смс-сообщения. После чего женщина сказала, что передаст информацию в Центральный банк и в полицию. В дальнейшем с потерпевшим связались лжесотрудники ЦБ РФ и полиции, обманув по вышеуказанной схеме, убедили взять кредиты в различных банках и

перевести их на якобы «безопасные счета» через банкоматы на общую сумму более двух миллионов рублей.

В другом случае по схожей схеме мошенник представился сотрудником «Почты России» и под предлогом доставки заказного письма убедил потерпевшего назвать код из смс-сообщения. Затем по известной схеме в «обработку» вступили лжесотрудники «Госуслуг», Центробанка и МВД, таким образом похитили 842 тысячи рублей у 49-летнего жителя г.Уфы.

*****

Самый действенный предлог из последних, который начал использоваться сравнительно недавно (с осени 2023 года) - мошенники, звонят жертве на телефон и, представляясь сотрудником оператора мобильной связи просят назвать код из СМС-сообщения, якобы для смены тарифного плана или подтверждения личности, и далее действуют по ранее отработанной вышеуказанной схеме (подключаются лжесотрудники банков). Код из СМС-сообщения мошенникам нужен для получения доступа к учетной записи (профилю) жертвы в личном кабинете «Госуслуги», мобильному банку, соцсети, а также для запугивания жертвы о том, что: «Вы недавно сообщили мошенникам код из СМС-сообщения, поэтому ваши деньги на банковском счет в опасности!!!».

Характерная фабула:

С заявлением обратилась жительница г.Уфы, 1965 года рождения, о том, что неизвестные мужчина и женщина, позвонив с абонентских номеров, представившись сотрудниками сотовой компании «Газпромбанк Мобайл», под предлогом обновления сим-карты, совершили хищение 5 млн. 575 тыс. рублей путем перевода

через мобильные приложения банков. После звонка мошенники посоветовали установить на ее мобильный телефон различные приложения, после чего потерпевшую попросили не отключать телефон и быть на связи, пока идет обновление. Далее потерпевшая заходила в свои приложения, где у нее были вклады. 19 октября потерпевшая обнаружила отсутствие своих накоплений.

Данные преступления отличается высокой анонимностью, так как злоумышленниками используются так называемые «подменные» номера зачастую реальных номеров банков и правоохранительных органов, размещенных на официальных сайтах. Технически установить настоящие абонентские номера, использовавшиеся при совершении преступлений, в основном не возможно, тем самым изначально отсутствует один из информационных следов преступления. Кроме этого, с развитием средств безналичного расчета денежные средства злоумышленники стараются переводить не на банковские счета, а на различные платежные системы, абонентские номера, криптовалютные счеты, где их движение сложно заблокировать и отследить.

*****

В настоящее время в связи с активным ростом рынка электронных платежей и онлайн-шопинга развиваются и новые современные формы мошенничества с использованием информационных технологий. Наиболее популярной схемой является фишинг. Это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей или банковским реквизитам. Фишинг может выражаться посредством

e-mail рассылок под видом известных сервисов, а также при поиске информации в интернете, при переходе на которые человек попадает на сайт, внешне неотличимый от настоящего. Когда пользователь вводит там свои данные, мошенники получают доступ к ним, после чего происходит хищение денежных средств.

Характерная фабула:

С заявлением обратилась гр-ка «Т», которая просит привлечь к уголовной ответственности не установленное лицо, которое под предлогом продажи сотового телефона похитило принадлежащие ей денежные средства в размере 20 800 руб. Установлено, что заявитель, увидев в сети «Интернет» на интернет сайте «Юла» объявление о продаже сотового телефона, связалась с продавцом по абонентскому номеру, после чего, продавец прислал ссылку на поддельный интернет сайт «www.youla.pay-delivery.ru», пройдя по которой заявитель перевела денежные средства в размере 10 400 руб. Продавец пояснил, что денежные средства не поступили на счет и попросил повторить операцию, после повторения заявителем операции, произошло повторное списание 10400 руб. В последующем продавец перестал выходить на связь.

Чтобы обезопасить от данного вида мошенничества, никогда не переходите по ссылкам от неизвестных вам лиц !!!

*****

Огромную проблему представляют мошенничества в сфере инвестиций. Под видом финансовых экспертов мошенники в интернете рассказывают об уникальной схеме заработка, обещают прибыль до 250% годовых. Дизайн мошеннических сайтов похож на

известные торговые площадки, данный сайт имитирует реальные биржи и может показывать данные реальных торгов. Как правило мошенники предлагают повышенную доходность. Обычные вклады в рублях приносят 4-5% годовых, мошенники, в свою очередь, обещают минимум 10-30% годовых, а иногда и доходность до 250% годовых. Мошенники даже создают личный кабинет жертвы, где транслируется выигрыш и заманчивый крупный баланс на счете. При этом после того, как потерпевший осуществит вклад денежных средств и захочет вывести прибыль, финансовые эксперты исчезают, денежные средства не возвращаются.

Например, в Отдел полиции №8 города Уфы поступило заявление от продавца магазина «Магнит», которая инвестировала в торговую площадку на иностранном сайте почти два с половиной миллиона рублей по совету финансового специалиста, с которым познакомилась по «Скайпу».

Поэтому не участвуйте в инвестировании организаций по объявлениям в Интернете, а если хотите вложить куда-то накопленные средства, то лучше обратитесь в официальное отделение любого банка !!!

*****

Регулярно встречается взлом аккаунтов и рассылка от друзей с целью наживы. Мошенники пишут в мессенджерах, на электронную почту или в социальные сети родственникам и знакомым владельца аккаунта (профиля) с просьбой срочно перевести денежные средства, придумывая различные предлоги. Зачастую потерпевшие, не

разобравшись в ситуации, сразу же переводят деньги неизвестным лицам.

Поэтому перед отправкой денег своему знакомому перезвоните ему по обычной телефонной связи или другому мессенджеру !!!

*****

Также хочется отметить, что в связи со сложившейся политической ситуацией в стране и в мире, мошенники помимо хищения денежных средств, заставляют граждан выполнять определенные действия, которые могут быть уголовно наказуемыми в нашей стране, например В мае 2023 года неустановленными лицами, под видом сотрудников службы безопасности банка ПАО «Сбербанк», посредством мессенджера «WhatsApp», совершены мошеннические действия в отношении гр. «И». В последующем, они же, под предлогом возврата похищенных денежных средств, склонили гр. «И» к передаче одной из схем эвакуации цеха оборонно-промышленного комплекса и совершению поджога отделения банка в г. Уфе. После выполненных условий, гражданину «И» сообщили, что он оказал содействие сотрудникам «ЦИПСО» Республики Украина (Центр информационно-психологических операций — украинское подразделение ВСУ, занимающееся кибератаками). По данному факту в отношении гр. «И» возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 213 УК РФ.

Аналогичные факты совершены в отношении жителей Учалинского и Янаульского районов, которых в результате взлома принадлежащих им страниц в социальной сети «ВКонтакте», под

угрозой распространения интимной переписки, склонили к распространению видеороликов, дискредитирующих действия ВС России.

Чтобы не попасть на уловки мошенников, нужно проявлять бдительность при совершении любых денежных операций с помощью банковских карт и никогда никому не раскрывать данные карты !!!

*****

До сих пор почти ежедневно в органы внутренних дел республики обращается хотя бы один работник бюджетной организации (учитель, налоговый инспектор, преподаватель ВУЗа или СУЗа, работник ГУПа, МУПа, даже сотрудник банковского учреждения). В 1-ом квартале текущего года профессора Башкирского ВУЗа мошенники «обчистили» на несколько миллионов рублей (потерпевший им поверил, потому что они представились ректором, разместив на «Аватаре» в «Ватсап» фотографию этого ректора).

Аналогичную хитрость совершили буквально на днях (10 сентября 2024 года) с врачом-рентгенологом одной из больниц города Уфы (потерпевшему пришло сообщение в «Ватсап» якобы от главврача (так подумал потерпевший, потому что на «Аватаре» была размещена фотография этого главврача) и потребовал в приказном порядке слушаться «сотрудников ФСБ и Сбербанка, чтобы не стать жертвой мошенников»). Ущерб составил 5 млн. 284 тыс. рублей.

*****

Особую обеспокоенность вызывают мошенничества, жертвами которых становятся пожилые граждане – под предлогом того, что **родственник попал, либо спровоцировал ДТП**. Несмотря на то, что способ давно устаревший, граждане, в подавляющем большинстве случаев пожилые люди, «клюют» на данную уловку. Здесь расчет сделан как раз на пожилых людей, так как звонки идут на стационарные телефоны, которыми в современном мире пользуются только пенсионеры, при этом их постоянно держат на телефоне и не дают опомниться. Злоумышленники с использованием мобильной связи, как правило, звонят на стационарный телефон пожилым гражданам, представляясь родственником, просят передать наличными денежными средствами курьерам или совершить банковские переводы за «решение вопроса» об уклонении от уголовной ответственности за якобы совершенное ДТП и компенсацию ущерба пострадавшим. Разговор с «лжеродственником» непродолжителен, затем вступает в разговор сотрудник правоохранительных органов, который подтверждает требование о вышеуказанной «компенсации», затем:

- потерпевший передает наличными денежными средствами свои сбережения присланному злоумышленниками курьеру, который впоследствии через банкомат зачисляет деньги на банковские счета злоумышленников;

- или потерпевший осуществляет перевод денежных средств по указанным злоумышленниками счетам.

Характерный пример:

Потерпевшей возрастом более 70 лет позвонили на стационарный телефон номер. Телефон без определителя, с какого номера звонили, сказать не может. Звонившая представилась дочерью потерпевшей, при этом не называя своих данных и данных потерпевшей, сообщила о том, что попала в ДТП, где является его виновником, и в результате которого пострадала водитель-девушка. В ходе телефонного разговора пояснили, что договорились о денежной компенсации в размере 800 тыс. рублей якобы на лечение пострадавших, на что потерпевшая ответила, что у нее нет таких денег, есть только 300 тыс. рублей наличными дома. Поверив неизвестной женщине, потерпевшая упаковала денежные средства, а также вещи личной гигиены в пакет, которые позже передала неизвестному мужчине, при этом не прекращая телефонного разговора.

Только, передав денежные средства, потерпевшая решила позвонить дочери и выяснить, все ли у нее в порядке.

*****

В г.Стерлитамаке зарегистрирован в текущем году факт телефонного мошенничества, совершенный под предлогом оказания экстрасенсорных услуг.

70-ти летняя потерпевшая по телевизионному каналу увидела программу «Восьмое чувство», заинтересовавшись, увидела номер телефона по бегущей строке и созвонилась с женщиной, которая представилась экстрасенсом Эльмирой. Выслушав проблему, «Эльмира» под предлогом проведения специальных обрядов убедила потерпевшую перевести 580 тысяч рублей.

*****

09 сентября 2024 года зарегистрирован первый факт мошенничества в республике, совершенный под предлогом замены счетчиков и установки приложения «Энергосбыт». Пенсионерке из города Уфы в «Ватсапе» позвонил неизвестный, представившись сотрудником Энергосбытовой компании сообщил, что ей необходимо заменить счетчик, а для этого нужно написать заявление. Для того, чтобы написать заявление, ее убедили установить на сотовый телефон онлайн приложение якобы «Энергосбыт», на что потерпевшая сбросила трубку. После чего телефон потерпевшей стал виснуть и перестал работать. Через 10 мин потерпевшая позвонила менеджеру банка ПАО «ВТБ» и попросила посмотреть, что у неё со счетом, так как телефон завис, на что менеджер ответил, что со счета потерпевшей были списание 900 тыс. рублей.

*****

Как правило, у отдельных работников профилактируемого предприятия возникают дополнительные вопросы, требующие для ответов дополнительное время, неустановленное регламентом встречи с трудовым коллективом.

Кроме того, телефонные мошенники регулярно обновляют свои предлоги для манипулирования потерпевшими, что не позволяет своевременно предупредить значительное количество граждан о новых способах обмана.

С целью максимального охвата населения материалами пропагандистского характера и актуального информирования о новых способах мошенничеств под личным кураторством начальника специализированного отдела по раскрытию мошенничеств

общеуголовной направленности и хищений, совершаемых с использованием информационно-телекоммуникационных технологий УУР МВД по РБ подполковника полиции Гузаирова М.Р. во взаимодействии с Пресс-службой МВД по РБ для профилактики мошенничеств создан общественный телеграмм-канал **«Мошки»: https://t.me/bashmoshki,** также аналогичное сообщество в соцсети «Вконтакте»: **vk.com/ bashmoshki** *(QR-код прилагается).*

*****

В окончание лекции прошу запомнить несколько простых правил, следуя которым Вы на 90% обезопасите себя от интернет-мошенников:

- не сообщать НИКОМУ данные своей банковской карты, а также коды из СМС-сообщений,

- не осуществлять какие-либо финансовые операции (снятие и зачисление наличных денежных средств, электронные переводы) по просьбе неизвестных Вам лиц, даже тех, которые представляются сотрудниками банков, МВД, ФСБ, Прокуратуры или Следственного комитета;

- перед отправкой денег своему знакомому перезвоните ему по обычной телефонной связи или другому мессенджеру;

- не участвовать в инвестировании организаций по объявлениям в Интернете;

- не переходить по неизвестным ссылкам в сети Интернет!!!

УУР МВД по РБ