Хищения, совершаемые под предлогом несанкционированного доступа к банковским счетам, злоумышленниками, представляющимися сотрудниками службы безопасности банков.

В последнее годы участились случаи хищений, при которых злоумышленники осуществляют звонки гражданам, представляясь при этом сотрудником службы безопасности банка и сообщают потерпевшему о несанкционированном доступе к его счету либо встречаются факты рассылки сообщений от имени банков, с различными текстами, «ваша карта заблокирована», «по вашей карте произведено списание денежных средств» и т.д. В дальнейшем, в ходе разговора мошенник просит назвать реквизиты банковской карты (*номер карты, срок действия, данные о владельце, код, указанный на оборотной стороне банковской карты*), чтобы якобы аннулировать операцию, однако в последующем названные данные использует при входе в мобильный банк, либо для осуществления перечислений на расчетные счета. При этом потерпевшим на мобильный телефон поступают смс сообщения, содержащие коды доступа или пароль на проведение операции, которые также просит назвать мошенник. Также, после получения доступа к счету, злоумышленник выясняет у потерпевшего сведения о имеющихся счетах в других банках и якобы переключая на сотрудника службы безопасности другого банка продолжает свой преступный умысел.

При данном способе обмана зачастую используются подменные номера, которые фактически оригинальны со справочными телефонами банковских учреждений и иными организациями, в том числе правоохранительными органами.

Ни при каких обстоятельствах не называйте пароли и коды доступа к банковским картам и счетам, указанным на оборотах карты и в смс – сообщениях, поступивших на телефон. Ни один из представителей банка не запросит данную информацию, а единственный достоверный номер телефона банка указан на обратной стороне банковской карты, либо договора заключенного в письменной форме.

Мошенничества, совершаемые при купле - продаже товаров на сайтах бесплатных объявлений («Авито», «Юла», «Из рук в руки»).

В данном случае можно выделить два способа совершения мошенничества:

1. Злоумышленники связываются с потерпевшим, разместившим объявление о продаже различного рода товаров, и в ходе разговора предлагают перечислить денежные средства на банковскую карту, в счет предоплаты. При согласии потерпевшего, злоумышленник просит назвать реквизиты банковской карты (*номер карты, срок действия, данные о владельце, код, указанный на оборотной стороне банковской карты*), которые в последующем использует при входе в мобильный банк, либо для осуществления перечислений на расчетные счета. При этом потерпевшим на мобильный телефон поступают смс сообщения, содержащие коды доступа или пароль на проведение операции, которые также просит назвать злоумышленник.

2. Злоумышленник размещает объявление о продаже товара по выгодной цене, которым в действительности не владеет (*зачастую мошенники создают копию объявления добросовестных продавцов, с аналогичными фотографиями и описанием товара*) и в ходе разговора с потерпевшим, под различными предлогами (*снижение цены, необходимости срочной продажи*) просит перевести денежные средства на банковскую карту (*всю сумму, либо часть суммы*), после чего обязуется отправить товар почтой, либо через транспортную компанию.

Чтобы обезопасить себя от таких преступлений, нельзя соглашаться на предоплату и покупку товара без его осмотра. Ни при каких обстоятельствах не называть пароли и коды доступа к банковским картам и счетам, указанным на оборотах карты и в смс – сообщениях, поступивших на телефон.

Мошенничества при покупке товара на сайтах интернет магазинов.

В данном случае в значительной степени используются сайты дубликаты (*двойники*), в названии (*домене*) которого имеется различие с оригиналом в одном символе. При этом содержание сайта полностью повторяет оригинал. Также встречаются сайты, которые не имеют аналогов и созданы они только с целью обмана граждан.

Не застрахованы от подобного рода обмана крупные организации и предприятия Республики, от имени которых мошенники действуют на всей территории России.

Чтобы не стать жертвой таких преступлений, необходимо проверять подлинность интернет сайтов, на которых осуществляется заказ того или иного товара, путем прочтения комментариев и отзывов, размещенных на просторах сети Интернет. Существует возможность проверить дату создания сайта на ресурсе reg.ru, в результате станет понятно, насколько долго данный сайт существует, как правило сайты, используемые мошенниками создаются незадолго до самого факта предоставления услуг, продажи товара.

Мошенничества, совершаемые под предлогом инвестирования, получения пассивного заработка, приобретения криптовалют и т.д.

В данном случае злоумышленники размещают на просторах сети различную «фишинговую» информацию о выгодном вложении денежных средств, инвестировании, торгах на фондовой бирже, и в ходе общения рассказывают о значительном заработке, что привлекает доверчивых граждан. В основном после получения денежных средств злоумышленники прекращают общения, но встречаются факты, когда обман происходит продолжительное время, при этом якобы неизвестные помогают в получении дохода, который частично удается получить, однако это сделано только для привлечения больших средств, но в итоге потерпевший лишается своих денежных средств. В таких случаях злоумышленники часто используют программы удаленного доступа «TeamViewer», «AnyDesk» и т.д., позволяющие на расстоянии использовать компьютер или телефон потерпевшего.

Чтобы не стать жертвой таких преступлений, необходимо использовать только официальные приложения для инвестирования (*в основном созданные кредитно-финансовыми учреждениями*), покупки и продажи криптовалют, а также добросовестных и проверенных организаций, так как в целом различные способы заработка обладают высокими рисками потери денежных средств.

Мошенничества в социальных сетях
«ВКонтакте», «Одноклассники», «Instagram», «Skype» и т.д.

В данном случае можно выделить три способа совершения мошенничества:

1. Злоумышленник, путем взлома страницы, осуществляют рассылку сообщений всему списку контактов, с различными текстами, которые зачастую начинаются с обычного приветствия. В случае ответа на сообщение, злоумышленник просит оказать материальную помощь, под различными предлогами (*необходимость оплаты услуг, оказание помощи больному родственнику)* и отправляет данные банковской карты, на которую нужно перечислить денежные средства.

В случае получения такого рода сообщений, обязательно необходимо связаться с лицом, которому принадлежит страница социальной сети, и уточнить, в действительности ли он отправил сообщение.

2. Продажа товаров в группах и страницах социальных сетей. Данный способ мошенничества схож с продажей товаров на сайтах бесплатных объявлений, при которых мошенник размещает объявление о продаже товара, которым в действительности не владеет и в ходе переписки с потерпевшим, просит перевести денежные средства на банковскую карту (*всю сумму, либо часть суммы*), после чего обязуется отправить товар почтой либо через транспортную компанию.

При заказе товара данным способом, проверяйте добросовестность продавца, путем прочтения комментариев и отзывов.

3. Мошенничества при знакомствах в социальных сетях сети Интернет. В данном случае злоумышленники в большинстве случаев представляются иностранцами и входе продолжительной переписки, входят в доверие потерпевших и в последующем под различными предлогами убеждают их перечислить денежные средства.

Мошенничества, совершаемые под предлогом
оказания помощи родственнику, попавшему в беду (ДТП).

В основном такой вид мошенничеств нацелен на пожилых и совершается лицами, отбывающими наказания в местах лишения свободы. При совершении данного вида мошенничества мошенник осуществляет случайный набор абонентских номеров (*городских, сотовых*) и в ходе телефонного разговора, представляется родственником (*сыном, внуком, зятем*), сообщает о том, что попал в ДТП (*при этом говоря взволнованным голосом*) и для решения проблемы ему необходимо срочно передать денежные средства сотруднику ГИБДД (следователю, дознавателю работнику прокуратуры и т.д.)

или потерпевшей стороне, путем перечисления денежных средств на счет мобильного телефона, либо передать их лицу, которое приедет за деньгами.

При поступлении такого рода звонков, обязательно свяжитесь с родственником, которым представляется мошенник, с целью уточнения его настоящего местонахождения. В случае, если у Вашего родственника не доступен абонентский номер, свяжитесь с совместно проживающими с ним родными и сообщите в полицию.

Мошенничества, совершаемые под предлогом компенсации за ранее приобретенные некачественные медицинские препараты (БАДы – биологические активные добавки).

В данном случае мошенники используют базы данных лиц, которые в действительности ранее приобретали такие препараты. В ходе телефонных разговор, неизвестные представляются сотрудниками правоохранительных органов (*прокуратуры, следственного комитета*), сообщают им, что они расследуют уголовное дело в отношении распространителей таких препаратов и им положена денежная компенсация. Далее, мошенники представляются работниками центрального банка и под различными предлогами (*оплата гос. пошлины, налога, курьерских услуг, процента за перечисление*) завладевают денежными средствами потерпевших, исчисляемые сотнями тысяч рублей, которые якобы в дальнейшем вернуться вместе с компенсацией.

Ни при каких обстоятельствах не перечисляйте денежные средства неизвестным лицам, ни один из представителей правоохранительных органов и банковских учреждений не потребует перечислить денежные средства. Компенсация причиненного вреда, как морального, так и материального возможна лишь по судебному решению, вступившему в законную силу, по заявлению которое было написано гражданином.

Общие правила безопасности, которые нужно соблюдать, чтобы не попасть на уловки мошенников:

В первую очередь необходимо быть более внимательным, узнавать больше о существующих мошеннических схемах (с этой целью МВД по РТ проводят большую работу по профилактике, выступая в различных средствах массовой информации, распространяя полиграфическую продукцию в различных местах массового пребывания граждан).

Убеждайтесь в достоверности информации, полученной в ходе телефонного разговора и интернет переписки с неизвестными, которые могут представляться родственниками, сотрудниками правоохранительных органов, представителями операторов сотовой связи и банковских учреждений, знакомыми и прочими лицами. Перезванивайте родственникам и знакомым, от чьего имени действуют незнакомцы;

В случае малейших подозрений немедленно сообщайте об этом в правоохранительные органы по телефону «02», «112».