

УМВД России на комплексе «Байконур»

УВЕДОМЛЕНИЕ!



УВАЖАЕМЫЕ ЖИТЕЛИ!

На территории города Байконур участились случаи мошенничеств и краж со счетов граждан! В целях предотвращения хищений с Ваших банковских карт рекомендуем ознакомиться с информацией на обороте данного уведомления.

БУДЬТЕ БДИТЕЛЬНЫ, НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ

<p>СИТУАЦИЯ 1.</p> <p>Вы получили СМС-сообщение о том, что Ваша банковская карта заблокирована, либо поступил звонок от «сотрудника банка», который сообщает о незаконных операциях по Вашему счету, предлагая пройти процедуру отмены незаконной операции и возврата похищенных денежных средств. В ходе разговора неизвестный пытается выяснить реквизиты банковских карт (номер, срок действия и код с оборотной стороны), а также коды, поступающие в СМС-сообщении.</p> <p>Никогда не перезванивайте на номер, указанный в тексте, или с которого поступило сообщение. Не отправляйте ответных сообщений. Не сообщайте никакую информацию по телефону неизвестному, даже если звонок поступил с «официального» номера кредитно-финансового учреждения.</p> <p>При возникновении подобной ситуации обратитесь в отделение банка лично, или позвонив по телефонному номеру, указанному в договоре обслуживания, а также на обороте платежной карты.</p>	<p>СИТУАЦИЯ 5.</p> <p>Общаетесь в Интернете и ведёте аккаунты в соцсетях? К Вам обратился знакомый с просьбой одолжить ему денежные средства, либо назвать свои данные карты для осуществления перевода?</p> <p>Никогда не переводите деньги на неизвестные Вам счета, предварительно не удостоверившись в том, что денежные средства требуются именно Вашему другу, связавшись с ним по телефону, даже если в сообщении он пишет, что не может говорить. Никогда не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред (фото паспорта и любых других документов). Общение в сети в значительной мере обезличено и за фотографией профиля может скрываться кто угодно.</p>
<p>СИТУАЦИЯ 2.</p> <p>Вы получили СМС, или ММС-сообщение со ссылкой на скачивание открытки, фотографии, музыки, картинки или программы.</p> <p>Никогда не переходите по ссылкам, поступающим в сообщениях. Перейдя по ссылке Вы, вероятнее всего, установите на устройство вредоносное программное обеспечение, которое в первую очередь нацелено на хищение денег с Вашего счета. Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.</p>	<p>СИТУАЦИЯ 6.</p> <p>Вам позвонили на телефон (сотовый или городской) под видом родственника и сказали, что попали в ДТП, в полицию и просят за решение вопроса перечислить денежные средства на карты, телефоны и др. счета.</p> <p>Помните, что прежде чем расстаться с деньгами, необходимо связаться с родственником под видом, которого звонят злоумышленники и убедиться, что с ним все в порядке. Также можно задать контрольный вопрос якобы родственнику (дата рождения, имя матери, адрес проживания) и злоумышленник сам закончит разговор.</p>
<p>СИТУАЦИЯ 3.</p> <p>Вы решили купить в Интернет-магазине, новый мобильный телефон, ноутбук, фотоаппарат, или любой другой товар по привлекательной цене, но сотрудник магазина просит перечислить предоплату.</p> <p>Никогда не перечисляйте деньги на электронные кошельки и счета мобильных телефонов. Помните, что интернет-магазин не может принимать оплату за покупку в такой форме. Если Вас просят оплатить товар с использованием терминалов экспресс-оплаты, или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.</p>	<p>СИТУАЦИЯ 7.</p> <p>Вам позвонил неизвестный либо пришел к Вам домой и предлагает различные услуги, в том числе оккультные (снятие порчи или сглаза, обмен денег в связи с предстоящей деноминацией, продажа препаратов, помогающих от всех болезней, и т.д.).</p> <p>В первую очередь предупредите своих родных и близких преклонного возраста, наиболее подверженных указанным преступным посягательствам, о мерах предосторожности в подобных ситуациях. Не открывайте дверь незнакомым людям. Если при этом они представляются работниками газовой службы, или любых других обслуживающих организаций – позвоните в данные учреждения, либо в полицию по телефонам: 02 – с городского, 102 – с мобильного.</p>
<p>СИТУАЦИЯ 4.</p> <p>Вы решили продать товар через сеть Интернет, после подачи объявления Вам звонит покупатель, сообщая о том, что готов оплатить товар, но для этого ему необходимо узнать реквизиты банковской карты для безналичного перевода (номер, срок действия и код с оборотной стороны), а также коды, поступающие в СМС-сообщении. Либо для получения оплаты необходимо выполнить определенные действия у банкомата.</p> <p>Никогда никому не сообщайте реквизиты карты, иначе денежные средства со счета будут похищены. Для перевода денег покупателю достаточно знать только номер карты, никакие другие сведения не требуются. Если Вас просят пройти к ближайшему банкомату, или терминалу оплаты, можете не сомневаться, Вы имеете дело с мошенником! Никогда не выполняйте указания неизвестного по телефону.</p>	<p>СИТУАЦИЯ 8.</p> <p>Вы в сети Интернет решили заработать при «игре» на бирже, инвестирования.</p> <p>Если Вы все - таки решили заработать данным видом, то следует играть на проверенных биржах, а также пользоваться услугами проверенных лиц (брокеров), занимающихся данной деятельностью. Также следует осознавать риск потери своих денежных средств при игре на бирже, инвестировании, в том числе очень крупных сумм.</p>
<p>СИТУАЦИЯ 9.</p> <p>Вам поступил звонок от «оператора сотовой связи», который сообщает, что абоненту необходимо переоформить договор об оказании услуг связи, поменять тарифный план на более выгодный, отключить платную услугу, иногда сообщают, что поступила заявка о смене мобильного оператора с сохранением номера и т.д. — в противном случае SIM-карта будет заблокирована. Для этого требуется назвать код из SMS, который приходит на номер абонента. На деле же в виде SMS приходит код подтверждения для входа в один из аккаунтов абонента.</p> <p>При поступлении такого телефонного звонка прервите разговор. Если вы продолжили общение и вам во время разговора пришел СМС-код от личного кабинета, никому не сообщайте его. Если возникли вопросы, самостоятельно позвоните в службу поддержки мобильного оператора по номеру, который указан на его официальном сайте.</p> <p>Помните, что мобильные операторы и сотрудники других структур не просят называть секретные коды из SMS. Более того, срок действия договора или действия SIM-карты не может истечь. Абоненту необходимо самостоятельно его расторгнуть или же это может сделать оператор, если клиент нарушил его правила или давно не пользовался номером.</p>	<p>СИТУАЦИЯ 10.</p> <p>Вам поступил звонок от «работника Почты» либо от «оператора курьерской службы», которые сообщают информацию о доставке на Ваше имя товара (посылки).</p> <p>Когда Вы сообщаете, что не заказывали никакой товар (посылку), Вам предлагают отказаться от получения, и чтобы подписать официальный отказ в базах нужно назвать код из СМС-сообщения.</p> <p>При поступлении такого телефонного звонка прервите разговор. Если вы продолжили общение и вам во время разговора пришел СМС-код, никому не сообщайте его и не вводите логин и пароль где бы то ни было по указанию неизвестных лиц.</p>

<p>СИТУАЦИЯ 11.</p> <p>Вам поступил звонок от «специалиста Роскомнадзора», который сообщает о необходимости замены приборов учета в принадлежащей вам квартире (счетчиков). Для этого требуется назвать код из SMS, который приходит на номер абонента, так как данный код является серийным номером прибора учета, который будет установлен. После выполнения указанного требования, на сотовый телефон поступают сообщения с портала государственных услуг Российской Федерации с кодами восстановления доступа к учетной записи.</p> <p>При поступлении такого телефонного звонка прервите разговор. Если вы продолжили общение и вам во время разговора пришел СМС-код, никому не сообщайте его и не вводите логин и пароль где бы то ни было по указанию неизвестных лиц.</p> <p>Помните, что войдя в личный кабинет портала «Госуслуги», злоумышленники, действуя от имени жертвы, регистрируются на сайтах микрофинансовых организаций, используя функцию «Войти с помощью «Госуслуг», затем оформляют кредит и обналичивают полученные деньги.</p>	<p>СИТУАЦИЯ 12.</p> <p>Вам поступил звонок от «сотрудника Социального фонда России», который сообщает, что по «новой информации» Вам не хватает стажа для пенсии, и пугают приостановкой выплат, если его не подтвердить. Злоумышленники предлагают записать Вас на прием в МФЦ, просят отсканировать и прислать личные документы, а затем подтвердить запись кодом по СМС.</p> <p>При поступлении такого телефонного звонка прервите разговор. Никогда не называйте звонящим по телефону паспортные данные, номер банковской карты, ПИН- или СМС-код или пароль от личного кабинета.</p> <p>Помните, что если возникает вопрос с перерасчетом стажа работы, то куда идти не нужно, сейчас все делается автоматически из электронных баз других ведомств. В крайнем случае, гражданину пришлют письмо, реальное, а не электронное. А звонить гражданину из Социального фонда России могут только в случае, если он подавал заявление, указывал телефон и по этому заявлению началась работа.</p>
<p>СИТУАЦИЯ 13.</p> <p>Ваши дети играют в разные мобильные или онлайн игры? Во многих онлайн-играх пользователям предлагается приобрести снаряжение, игровые бонусы для «прокачки» до максимального уровня или разблокировать какие-то новые локации. Однако не все эти покупки безопасны. Зачастую злоумышленники маскируют свой профиль под аккаунт ребенка в социальных сетях, на форумах или в онлайн-играх. Вашим детям может казаться, что они общаются со сверстником, а на самом деле это может быть взрослый человек или мошенник. Нередки случаи, когда такие виртуальные «друзья» могут подговорить ребенка сфотографировать и отправить им платежную карту родителей, продиктовать SMS-код, который придет на телефон или скачать вредоносное приложение.</p> <p>В первую очередь наладьте диалог со своим ребенком, беседуйте с ним о его виртуальных друзьях, как если бы речь шла о друзьях в реальной жизни. Объясните ребенку, почему нельзя доверять незнакомым людям, особенно в интернете, и какие данные нельзя раскрывать.</p> <p>А лучше всего не давать детям играть на своем телефоне, если к нему привязаны банковские карточки, особенно зарплатная карта, или хранится другая важная информация. Также стоит установить ограничения на покупки с телефонов и регулярно проверять платные подписки, которые ребенок может оформить случайно.</p> <p>Детям постарше, которым родители оформили свою банковскую карту, и имеющим собственный гаджет, надо объяснить, какие могут быть последствия, если скачивать сомнительные приложения. Лучше всего совершать все онлайн-покупки с помощью отдельной платежной карты, не привязанной к зарплатной, на которую следует закинуть только ту сумму, которую собираетесь потратить, и только на проверенных сайтах, скачивать приложения из официальных магазинов.</p>	<p>СИТУАЦИЯ 14.</p> <p>Вам поступил звонок от человека, умоляющего Вас срочно вернуть деньги, которые он случайно перевел вам по ошибке. Вы заходите в приложение банка или онлайн-кабинет и видите, что вам действительно пришла на счет указанная сумма.</p> <p>После просьбы потенциальной жертве вернуть эти деньги, мошенник обращается в банк, чтобы отменить свой перевод и таким образом возвращает свои деньги и получает новые от того, кому переводил средства или злоумышленники могут отправить фальшивое SMS-сообщение от банка с подменных номеров о зачислении на Ваш счет денег (в этом случае деньги на счет жертвы вообще не поступают).</p> <p>При поступлении такого телефонного звонка прервите разговор. Всегда при поступлении на карту неизвестных денег и последующих звонков их вернуть, нужно удостовериться, что перевод осуществлен на самом деле. Необходимо проверить баланс счета и обязательно проинформировать банк о поступлении чужих средств.</p> <p>Центральный банк не рекомендует самостоятельно возвращать деньги, полученные от незнакомца, а также тратить деньги, полученные от незнакомцев. Поскольку это действие может быть расценено как преступление.</p>

При поступлении сомнительных звонков от различных организаций и должностных лиц, а также при осуществлении операций по банковским картам, в совершении которых есть сомнения, Вы можете проконсультироваться в мессенджере WhatsApp со старшим оперуполномоченным отдела уголовного розыска по номеру телефона 87713174501 – Гуськов Иван Витальевич.