С начала 2019 года (по конец мая) лангепасцы перечислили на счета злоумышленников более 700 000 рублей. Всего за указанный период зарегистрировано 14 фактов мошенничества.

Риску посягательств мошенников подвержены в равной мере все категории граждан. Так, граждане пожилого возраста чаще реагируют на звонки с сообщениями о блокировке карты или о том, что родственник попал в беду. Трудоспособное население часто продает/покупает товары в интернете, не удостоверившись в репутации продавца или сайта и, таким образом, совершает сделку со злоумышленниками, при этом граждане самостоятельно переводят средства в виде предоплаты предполагаемому продавцу либо, поддавшись на уговоры, предоставляют злоумышленникам возможность доступа к своему онлайн-кабинету, привязанному к банковской карте.

ВИДЫ МОШЕННИЧЕСТВА И СПОСОБЫ ЗАЩИТЫ

В повседневной жизни гражданами используется множество разнообразных высокотехнологичных устройств – пластиковых карт, мобильных телефонов и компьютеров. Постоянно появляются новые модели, программы и сервисы. Все это делает нашу жизнь удобнее, но требует определённых навыков и знаний. Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан. Чтобы не поддаться на уловки злоумышленников, достаточно знать, как они действуют, и соблюдать правила пользования мобильными телефонами, пластиковыми картами и компьютерами.

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО. Основные схемы

Обман по телефону: требование выкупа

КАК ЭТО ОРГАНИЗОВАНО:

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления.

Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Для решения вопроса необходима определенная сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

В организации обмана по телефону с требованием выкупа участвуют несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам. Нередко жертва сама случайно подсказывает имя того, о ком она волнуется. Если жертва преступления поддалась на обман и согласилась привезти указанную сумму, звонящий называет адрес, куда нужно приехать. Часто мошенники предлагают снять недостающую сумму в банке и сопровождают жертву лично. Мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег.

После того как гражданин оставляет деньги в указанном месте или кому-то их передает, ему сообщают, где он может увидеть своего родственника или знакомого.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Первое и самое главное правило — прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Хотя беспокойство за родственника или близкого человека мешает мыслить здраво, следует понимать: если незнакомый человек звонит Вам и требует привезти на некий адрес денежную сумму – это мошенник. Если Вы получили звонок от якобы близкого родственника или знакомого с информацией о том, что он попал в неприятную ситуацию, в результате которой ему грозит возбуждение уголовного дела, и если звонящий просит передать взятку якобы сотруднику правоохранительных органов, готовому урегулировать вопрос, следует задать уточняющие вопросы: «А как я выгляжу?» или «Когда и где мы виделись последний раз?», т.е. задавать вопросы, ответы на которые знаете только вы оба. Если вы разговариваете якобы с представителем правоохранительных органов, спросите, из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и поинтересоваться, действительно ли родственник или знакомый доставлен туда.

SMS-ПРОСЬБА О ПОМОЩИ

SMS-сообщения позволяют упростить схему обмана по телефону. Такому варианту мошенничества особенно трудно противостоять пожилым или слишком юным владельцам телефонов. Дополнительную опасность представляют упростившиеся схемы перевода денег на счёт.

КАК ЭТО ОРГАНИЗОВАНО:

Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

Телефонный номер-грабитель. Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества.

КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того как Вы перезваниваете, Вас долго держат на линии. Когда это надоедает, Вы отключаетесь – и оказывается, что с Вашего счёта списаны крупные суммы.

НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:

Существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:

Не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

ТЕЛЕФОННЫЕ ВИРУСЫ

Очень часто встречается форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.
Другой вид мошенничества выглядит так. При заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер ..., для подтверждения операции, отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства. Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт они снимаются с телефона.
Не следует звонить по номеру, с которого отправлено SMS – вполне возможно, что в этом случае с Вашего телефона будет автоматически снята крупная сумма.
Существует множество вариантов таких мошенничеств. Будьте бдительны!

ВЫИГРЫШ В ЛОТЕРЕЕ

В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей, особенно с участием радиостанций, мошенники часто используют их для прикрытия своей деятельности и обмана людей.
«Вы победили, сообщите код карты»
«Вы выиграли машину, нужны деньги для её оформления»
Выигрыш приза может стать не только приманкой, но и поводом затребовать перечисления крупных денежных средств для оформления нужных документов.
КАК ЭТО ОРГАНИЗОВАНО:
На Ваш мобильный телефон – как правило, в ночное время – приходит SMS-сообщение, в котором говорится о том, что в результате проведенной лотереи Вы выиграли автомобиль. Чаще всего это Audi A6, но упоминаются и другие известные иностранные модели и марки.
Для уточнения всех деталей Вас просят посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонных номеров.
Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности: уплатить госпошлину и оформить необходимые документы. Для этого необходимо перечислить на счет своего мобильного телефона определенную сумму, а затем набрать комбинацию цифр и символов якобы для проверки поступления денег на счет и получения «кода регистрации».
НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:
Комбинация цифр и символов, которую Вы набираете, на самом деле является кодом, благодаря которому злоумышленники получают доступ к перечисленным средствам. Как только код набран, счет обнуляется, а мошенники исчезают в неизвестном направлении.
КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:
Если Вы узнали о проведении лотереи только в момент «выигрыша», и при этом ранее Вы не заполняли заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то, вероятнее всего, Вас пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводится только по телефону и Интернету.

МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

Банковская карта – это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.
КАК ЭТО ОРГАНИЗОВАНО:

Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определенный номер для получения подробной информации.
Когда Вы звоните по указанному телефону, Вам сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.
НА САМОМ ДЕЛЕ ПРОИСХОДИТ СЛЕДУЮЩЕЕ:
Чтобы ограбить Вас, злоумышленникам нужен лишь номер Вашей карты и ПИН-код. Как только Вы их сообщите, деньги будут сняты с Вашего счета.
КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:
Не торопитесь сообщать реквизиты вашей карты! Ни одна организация, включая банк, не вправе требовать Ваш ПИН-код! Для того чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка. Скорее всего, Вам ответят, что никаких сбоев на сервере не происходило, а Ваша карта продолжает обслуживаться банком.

Владельцам пластиковых банковских карт
Как защититься от мошенников
В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. ОМВД России по г. Лангепасу рекомендует всем владельцам пластиковых карт следовать правилам безопасности:
ПИН-КОД – КЛЮЧ К ВАШИМ ДЕНЬГАМ
Никогда и никому не сообщайте ПИН-код Вашей карты.
Лучше всего его запомнить.
Относитесь к ПИН-коду как к ключу от сейфа с вашими средствами.
Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.
ВАША КАРТА – ТОЛЬКО ВАША
Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.
НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД
Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники. Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.
НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ ПРИ ЕЕ УТЕРЕ
Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.
ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ
При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.
Граждане, пользующиеся банкоматами без видеонаблюдения, могут подвергнуться нападениям злоумышленников.
ОПАСАЙТЕСЬ ПОСТОРОННИХ
Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей.
Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

Набирая ПИН-код, прикрывайте клавиатуру рукой.
Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.
БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»
Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.
БАНКОМАТ ДОЛЖЕН БЫТЬ ПОЛНОСТЬЮ ИСПРАВНЫМ
В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.
СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ
Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах. Свяжитесь с Вашим банком – он обязан предоставить консультационные услуги по работе с картой.
НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ
В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

ПОКУПКА/ПРОДАЖА ТОВАРОВ НА САЙТАХ ОБЪЯВЛЕНИЙ (Авито, Юла и т.п.)

Очень часто единственная цель мошенников на сайте объявлений это не покупка или продажа товаров, а просто способ узнать секретную информацию о вашей банковской карте.
Используя различные запутанные истории (перечислять все возможные легенды тут не имеет смысла, но поверьте, мошенники бывают очень изобретательны) вас вынуждают продиктовать код подтверждения, который приходит вам на телефон при входе в систему онлайн банкинга.
Таким образом, мошенники получают полный доступ к вашему банковскому счет и могут за считанные минуты похитить все имеющиеся на вашем счету средства.
Также иногда мошенники утверждают, что не могут перевести вам средства, пока вы не сообщите им секретный код (cvv), указанный на обороте вашей банковской карты.
Запомните: единственная информация, которая может быть нужна от вас покупателю – номер вашей банковской карты. 16 цифр, написанных на лицевой стороне. Все. Попытки получить какие-либо другие данные, скорее всего, свидетельствуют о мошенничестве.
Отдельные вид мошенничества в данном случае – заставить доверчивого продавца не выставить счет за товар, а наоборот, перечислить эту же сумму на счет мошенников. Для этого они просят вас обязательно подойти к банкомату и диктуют вам сложную последовательность действий, которая приводит к тому, что вы переводите мошенникам деньги.