ПАМЯТКА для граждан о профилактике и предупреждении дистанционных преступлений в сфере информационно-телекоммуникационных технологий:

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно-телекоммуникационных технологий стремительно набирают силу.

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе либо совершать те или иные действия, используют человеческие слабости (стяжательство, алчность), чувства (сострадание, обеспокоенность за близких, жалость) в своих корыстных интересах.

Основные известные схемы телефонного мошенничества:

1. Случай с родственником.

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение преступления (совершил ДТП, хранил оружие или наркотики, нанёс тяжкие телесные повреждения). Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз «помогал» людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас деньги необходимо привезти в определенное место, передать какому-либо человеку, либо перевести на счет (абонентский номер телефона).

2. Розыгрыш призов (это могут быть телефон, ноутбук, автомобиль и др.).

На телефон абонента сотовой связи приходит смс-сообщение, из которого следует, что в результате проведенной лотереи он выиграл автомобиль. Для уточнения всех деталей потенциальной жертве предлагается посетить определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из указанных телефонных номеров. Во время разговора по телефону мошенники сообщают о том, что для выполнения необходимых формальностей (уплаты госпошлины, оформления необходимых документов, оплаты за комиссию перевода) счастливому обладателю новенького автомобиля необходимо перечислить на счет указанную ими сумму, а затем набрать определенную комбинацию цифр и символов, якобы для проверки поступления денег на счет и получения «кода регистрации». Как только жертва завершает указанные манипуляции, счет обнуляется, а мошенники исчезают в неизвестном направлении.

Если вы узнали о проведении лотереи только тогда, когда «выиграли» автомобиль, если вы не заполняли заявку на участие в ней либо каким-либо другим способом не подтверждали свое участие в розыгрыше, то, вероятнее всего, вас пытаются обмануть. Будьте осторожны!

3. SMS-просьба.

Абонент получает на мобильный телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если номер не доступен, положи на него определенную сумму и перезвони». Человек пополняет счёт и перезванивает, телефон по-прежнему не доступен, а деньги вернуть уже невозможно.

4. Телефонный заказ от руководителей правоохранительных и государственных органов власти.

На телефон абонента (предпринимателя, руководителя объекта общественного питания, торгового центра либо их сотрудникам и др.) поступает звонок от правонарушителя, который представляется одним из руководителей правоохранительных органов (прокуратуры города и др.) и просит пополнить счет его телефона, дополнительно к этому просит, например, забронировать столик в ресторане и сообщает, что по приезду на объект рассчитается. Не дожидаясь приезда якобы должностного лица, руководствуясь принципом уважения и доверия к руководителю названной должности в правоохранительных органах, потерпевший переводит через терминал банка, либо через иные финансовые услуги денежные средства в указанной сумме.

5. Платный код.

Поступает звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи, с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для

осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

6. Штрафные санкции оператора.

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (также могут быть варианты: не внес своевременную оплату, воспользовался услугами роуминга без предупреждения) и, соответственно, ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды.

7. Ошибочный перевод средств.

Абоненту поступает SMS-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина (или женщина) сообщает, что ошибочно перевел деньги на его счет, при этом просит вернуть их обратно тем же «Мобильным переводом». В действительности деньги не поступают на телефон, а человек переводит свои собственные средства. Если позвонить по указанному номеру, он может быть вне зоны доступа. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.

8. Предложение получить доступ к СМС-переписке и звонкам абонента.

Учитывая склонность некоторых граждан «пошпионить» за близкими и знакомыми, злоумышленниками используется следующая схема мошенничества в сети Интернет: пользователю предлагается изучить содержание смс-сообщений и список входящих и исходящих звонков интересующего абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 рублей на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента.

После того, как пользователь отправляет смс, с его счета списывается сумма гораздо больше той, что была указана мошенниками, а интересующая информация впоследствии так и не поступает.

9. Продажа имущества на интернет-сайтах.

При звонке на телефон, размещенный на Интернет-сайтах объявлений (Авито, ФарПост, Дром и др.) правонарушитель просит пополнить счет его телефона, либо сообщить данные и номер карты потерпевшего для перевода денежных средств в качестве задатка за товар. После сообщения данных карты происходит списание денежных средств.

10. Новая схема телефонного мошенничества «Вишинг».

Одной из распространенных схем киберпреступников в последние годы стал «Вишинг» – это вид мошенничества, при котором злоумышленники под любым предлогом вынуждают нас предоставлять конфиденциальные данные в «наших собственных интересах», то есть искусственно создается ситуация, требующая помощи от специалиста.

Цель мошенников под любым предлогом извлечь секретную личную информацию о кредитке. Для получения доступа к конфиденциальным данным владельца мнимые помощники используют телефонную связь как в автоматизированном режиме, так и напрямую от мнимого «операциониста» банковского сектора.

Во многих случаях в течение дня нам постоянно начинают звонить на мобильник с незнакомого московского номера, начинающегося на 495. Звонки с московских номеров обычно настолько настойчивы (иногда до десяти звонков за день), что мы зачастую уступаем и отвечаем на них.

Как только мы отвечаем на звонок, нам сразу сообщают важную информацию о возникших проблемах с нашей картой, например, что она заблокирована, а служба безопасности банка предотвратила попытку несанкционированного списания. Затем звонящий предлагает помощь в сложившейся ситуации, на которую многие из нас соглашаются.

Нас убеждают в срочном решении возникшей ситуации, пока еще не все деньги украдены. Очень последовательно мошенники стараются получить от нас всю личную информацию о кредитке, присылают новые пароли и ПИН коды в СМС-уведомлениях. Успокаивающим голосом «банковские работники» предлагают различные возможные варианты защиты.

Догадаться о том, что любезный помощник на другом конце провода является мошенником не всегда легко, но в любом случае это возможно. Изначально можно поблагодарить за бдительность

и узнать должность, инициалы звонившего сотрудника кредитной организации и предпринять попытку дозвониться по горячей линии.

Использовать для выяснения сложившейся ситуации лучше другой свой номер, потому что на сегодняшний день у вымогателей существуют технологии, позволяющие перенаправлять все последующие звонки на телефонное устройство мошенников.

11. Хищения с карт, подключенных к опции бесконтактных платежей.

Для проведения оплаты по такой карте достаточно приложить её к терминалу. Ввод ПИН-кода не требуется если сумма не превышает 1 000 рублей. При этом количество расходных транзакций не ограничено.

Чтобы получить деньги, мошеннику даже не понадобится воровать карту у клиента. Если в общественном транспорте поднести устройство к сумке или карману владельца, то средства спишутся. Для этих целей мошенники изготавливают самодельные переносные считыватели или используют банковские терминалы, оформленные по фиктивным документам.

Также в текущем году злоумышленники продолжают активно использовать фишинг в социальных сетях и онлайн-мессенджерах. Наибольшую выгоду мошенникам приносят махинации через Авито, с помощью которых они получают доступ в онлайн-банк.

12. Взлом аккаунта друга.

Люди могут даже не подозревать, что им пишет посторонний человек под видом родственника, друга, с просьбой перевода денег в связи с произошедшим горем. Таким образом, войдя в доверие, мошенники пытаются украсть ваши деньги.

13. Телефонное мошенничество во время пандемии.

Многие из нас ввиду пандемии находились дома, что активизировало мошенничество с банковскими картами по телефону. Очень оперативно этим моментом воспользовались вымогатели с помощью смартфона.

Вот лишь несколько новых примеров того, как происходит телефонное мошенничество с последующей кражей денег с кредитки, учитывая современную ситуацию:

· на телефон приходит СМС-уведомление о начислении компенсации за нерабочий период во время эпидемии, для получения которой предлагается перезвонить в банк и пообщаться с мнимым «сотрудником».

· злоумышленники звонят нам с уведомлением о том, что мы якобы находились в контакте с заболевшими Covid-19. В связи с этим предлагается срочно сдать платный анализ на коронавирус, а чтобы не нарушать режим самоизоляции, «сотрудники лаборатории» готовы приехать к нам на дом. Для срочного выезда бригады нужно совершить предоплату.

В обоих случаях подставной человек, будь это сотрудник банка или мед. персонал, предлагает свою онлайн-помощь, чтобы осуществить платеж, а для этого ему нужна информация о счете. После получения необходимых данных мошенники выводят деньги, а мы, доверчивые граждане, остаемся с нулевым балансом.

Приведенный перечень мошеннических схем не ограничивается приведенными примерами. Преступники находят все новые и новые схемы и способы для достижения своих преступных замыслов.

Как уберечься от телефонных мошенничеств?

Чтобы не стать жертвой злоумышленников, необходимо соблюдать простые правила безопасного поведения и обязательно довести их до сведения родных и близких:

– не следует доверять звонкам и сообщениям, о том, что родственник или знакомый попал в аварию, задержан сотрудниками полиции за совершение преступления, особенно, если за этим следует просьба о перечислении денежных средств. Как показывает практика, обычный звонок близкому человеку позволяет развеять сомнения и понять, что это мошенники пытаются завладеть вашими средствами или имуществом;

– не следует отвечать на звонки или SMS-сообщения с неизвестных номеров с просьбой положить на счет деньги;

– не следует сообщать по телефону кому бы то ни было сведения личного характера.

Своевременное обращение в правоохранительные органы может помочь другим людям не попасться на незаконные уловки телефонных мошенников.

Противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием и бдительностью.

ПАМЯТКА для граждан о профилактике и предупреждении дистанционных преступлений в сфере информационно-телекоммуникационных технологий:

Чтобы не оказаться жертвой мошенников необходимо знать следующее:

– сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;

– не при каких обстоятельствах не сообщать данные вашей банковской карты, а так же секретный код на оборотной стороне карты;

– хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;

– не сообщать пин-код третьим лицам;

– остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;

– лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;

– внимательно читайте СМС сообщения приходящие от банка;

– никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;

– помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС сообщении от банка;

– сотрудники банка никогда не попросят вас пройти к банкомату;

– если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

– не покупайте в интернет – магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;

– никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

– в сети «Интернет» не переходите по ссылкам на неизвестные сайты;

– действуйте обдуманно, не торопливо, помните, что «Бесплатный сыр только в мышеловке».

Интернет-мошенничество – памятка для граждан
В последние годы широкую популярность получили смс-рассылки или электронные письма с сообщениями о выигрыше автомобиля либо других ценных призов. Для получения «выигрыша» злоумышленники обычно просят перевести на электронные счета определенную сумму денег, мотивируя это необходимостью уплаты налогов, таможенных пошлин, транспортных расходов и т.д. После получения денежных средств они перестают выходить на связь либо просят перевести дополнительные суммы на оформление выигрыша.

Оградить себя от подобного рода преступлений предельно просто. Прежде всего необходимо быть благоразумным. Задумайтесь над тем, принимали ли вы участие в розыгрыше призов? Знакома ли вам организация, направившая уведомление о выигрыше? Откуда организаторам акции известны ваши контактные данные? Если вы не можете ответить хотя бы на один из этих вопросов, рекомендуем вам проигнорировать поступившее сообщение.

Если вы решили испытать счастье и выйти на связь с организаторами розыгрыша, постарайтесь получить от них максимально возможную информацию об акции, условиях участия в ней и правилах ее проведения. Помните, что упоминание вашего имени на Интернет-сайте не является подтверждением добропорядочности организаторов акции и гарантией вашего выигрыша.

Любая просьба перевести денежные средства для получения выигрыша должна насторожить вас. Помните, что выигрыш в лотерею влечет за собой налоговые обязательства, но порядок уплаты налогов регламентирован действующим законодательством и не осуществляется посредством перевода денежных средств на электронные счета граждан и организаций или т.н. «электронные кошельки».

Будьте бдительны и помните о том, что для того, чтобы что -то выиграть, необходимо принимать участие в розыгрыше. Все упоминания о том, что ваш номер является «счастливым» и оказался в списке участников лотереи, являются, как правило, лишь уловкой для привлечения вашего внимания.

Нередки случаи мошенничеств, связанных с деятельностью Интернет-магазинов и сайтов по продаже авиабилетов. Чем привлекают потенциальных жертв мошенники? Прежде всего – необоснованно низкими ценами. При заказе товаров вас попросят внести предоплату, зачастую путем внесения денежных средств на некий виртуальный кошелек посредством терминала экспресс-оплаты. Далее магазин в течение нескольких дней будет придумывать отговорки и обещать вам скорую доставку товара, а потом бесследно исчезнет либо пришлет некачественный товар.

Цель подобных сайтов – обмануть максимальное количество людей за короткий срок. Создать Интернет-сайт сегодня – дело нескольких минут, поэтому вскоре после прекращения работы сайт возродится по другому адресу, с другим дизайном и под другим названием.

Если вы хотите купить товар по предоплате помните, что серьезные Интернет-магазины не будут просить вас перечислить деньги на виртуальный кошелек или счет мобильного телефона. Поищите информацию о магазине в сети Интернет, посмотрите, как долго он находится на рынке. Если вы имеете дело с сайтом крупной или известной вам компании, убедитесь в правильности написания адреса ресурса в адресной строке вашего браузера. При необходимости потребуйте от администраторов магазина предоставить вам информацию о юридическом лице, проверьте ее, используя общедоступные базы данных налоговых органов и реестр юридических лиц. Убедитесь в том, что вы знаете адрес, по которому вы сможете направить претензию в случае, если вы будете недовольны покупкой.

Заметно участились случаи рассылки смс-сообщений, содержащих информацию о том, что банковская карта абонента заблокирована в силу ряда причин. Иногда подобные сообщения содержат призыв перевести деньги для разблокировки карты, иногда абонента просят позвонить или отправить смс на короткий номер.

Необходимо помнить о том, что единственная организация, которая сможет проинформировать вас о состоянии вашей карты – это банк, обслуживающий ее. Если у вас есть подозрения о том, что с вашей картой что –то не в порядке, если вы получили смс-уведомление о ее блокировке, немедленно обратитесь в банк. Телефон клиентской службы банка обычно указан на обороте карты. Не звоните и не отправляйте сообщения на номера, указанные в смс-уведомлении, за это может взиматься дополнительная плата.

Один из популярных способов мошенничеств, основанных на доверии связан с размещением объявлений о продаже товаров на электронных досках объявлений и интернет-аукционах. Как правило, мошенники привлекают своих жертв заниженными ценами и выгодными предложениями и требуют перечисления предоплаты путем перевода денежных средств на электронный кошелек.

Благоразумие поможет и здесь. Внимательно изучите объявление, посмотрите информацию о лице, разместившем его. Если торговая площадка имеет систему рейтингов продавцов, изучите отзывы, оставленные другими покупателями, не забывая, однако, о том, что преступники могут оставлять положительные отзывы о себе, используя дополнительные учетные записи. Воспользуйтесь Интернет-поиском. Иногда достаточно ввести в форму поиска телефонный номер или сетевой псевдоним продавца для того, чтобы обнаружить, что эти данные уже использовались в целях хищения денежных средств и обмана покупателей.

Посмотрите среднюю стоимость аналогичных товаров. Чересчур низкая стоимость должна вызвать у вас подозрение. Если продавец требует перечислить ему полную или частичную предоплату за приобретаемый товар на электронный счет, подумайте, насколько вы готовы доверять незнакомому человеку. Помните, что перечисляя деньги незнакомым лицам посредством анонимных платежных систем, вы не имеете гарантий их возврата в случае, если сделка не состоится.

Покупать авиабилеты через Интернет удобно. Вам не нужно никуда ехать и стоять в очередях. Вы выбираете рейс, дату, оплачиваете билет и получаете его спустя несколько секунд. Сегодня многие люди выбирают именно такой способ приобретения билетов на самолет.

Естественно, мошенники не могут оставить данную сферу без внимания. За последний год существенно увеличилось количество жалоб на обман при покупке электронных билетов. Создать Интернет-сайт по продаже авиабилетов – дело нескольких часов, на смену его названия, адреса и внешнего оформления требуется еще меньше времени. Как правило, обман раскрывается не сразу, некоторые узнают о том, что их билетов не существует, лишь в аэропорту. Это дает мошенникам возможность перенести свой Интернет-ресурс на новое место и продолжать свою преступную деятельность под другим названием.

Чтобы не испортить себе отдых или деловую поездку стоит внимательно отнестись к покупке авиабилетов через сеть Интернет. Воспользуйтесь услугами Интернет-сайта авиакомпании или агентства по продаже билетов, давно зарекомендовавшего себя на рынке. С осторожностью отнеситесь к деятельности неизвестных вам сайтов, особенно тех, которые привлекают ваше внимание специальными предложениями и низкими ценами. Не переводите деньги на электронные кошельки или счета в зарубежных банках. Не поленитесь позвонить в представительство авиакомпании, чтобы убедиться в том, что ваш рейс существует и билеты на него еще есть. Эти простые правила позволят вам сэкономить деньги и сберечь нервы.

Если вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или какой -нибудь программы, не спешите открывать её. Перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.

Посмотрите, с какого номера было отправлено вам сообщение. Даже если сообщение прислал кто -то из знакомых вам людей, будет не лишним дополнительно убедиться в этом, ведь сообщение могло быть отправлено с зараженного телефона без его ведома. Если отправитель вам не знаком, не открывайте его.

Помните, что установка антивирусного программного обеспечения на мобильное устройство – это не прихоть, а мера позволяющая повысить вашу безопасность.