Комитет финансов города Курска

в целях повышения уровня защищенности граждан от хищений, совершаемых с использованием информационно-телекоммуникационных технологий, подготовил информационный материал на тему:

«Осторожно мошенники! Предупреждение дистанционных преступлений в сфере информационно-телекоммуникационных технологий»

Председатель
комитета финансов города Курска Стекачев В.И.

Курск , март 2022 г.

Сегодня в нашей повседневной жизни используется множество разнообразных высокотехнологичных устройств – пластиковых карт, мобильных телефонов, компьютеров, планшетов и других «умных» гаджетов. Постоянно появляются новые модели, программы и сервисы.

Все это делает нашу жизнь удобнее, но требует определенных навыков и знаний.

Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие обмануть и присвоить денежные средства граждан.

Чаще всего жертвами мошенников становятся наиболее незащищенные слои населения (лица преклонного возраста, пенсионеры, подростки),а так же лица, не обладающие навыками пользования компьютерными и мобильными техническими устройствами, не владеющие финансовой грамотностью.

В целях повышения эффективности противодействия хищениям, совершенным с использованием информационно-телекоммуникационных технологий и защиты граждан от подобных преступлений комитетом финансов города Курска разработана информационная памятка о наиболее распространенных способах обмана по телефону и кражи денег с банковских карт.

Телефонное мошенничество

Данный вид мошенничества известен давно и возник вскоре после массового появления телефонов.

В настоящее время он является одним из самых распространенных, так как мобильные телефоны используются всеми, начиная от детей и заканчивая пенсионерами.

Однако чаще всего на уловки телефонных мошенников попадаются доверчивые и пожилые люди.

Чтобы не стать жертвой мошенников достаточно следовать простым правилам безопасности.

Для этого разберем наиболее распространенные схемы телефонных мошенничеств.

Наиболее распространенные схемы телефонного мошенничества:

- «Родственник в беде»
- «SMS – сообщение о помощи»
- «Телефонные вирусы»
- «Обновление браузера»
- «Розыгрыш призов»
- «Мошенничество с банковскими картами»

Требование денежных средств за освобождение родственника или знакомого от ответственности («Родственник в беде»)

Как это работает.

На ваш телефон поступает звонок от неизвестного лица, который представляется вашим знакомым или родственником. Взволнованным голосом сообщает, что сотрудники полиции задержали его и обвиняют в совершении преступления. Как правило это совершение дорожно-транспортного происшествия с жертвами, хранение оружия или наркотиков.

После чего с вами начинает разговаривать другой человек, который представляется сотрудником полиции и сообщает, что знает, как можно решить вопрос за деньги, которые нужно привезти в назначенное место или передать другому человеку.

Что происходит на самом деле.

В данной схеме обмана участвуют несколько злоумышленников, набирая телефонные номера наугад и произнося заранее заготовленную фразу, а далее действуя по обстоятельствам. Очень часто жертва обмана сама неосознанно упоминает имя того, о ком волнуется . После чего, если она поддалась на уловки и согласилась передать деньги, мошенники называют адрес, куда необходимо приехать. При этом, запугивают жертву, не давая ей времени подумать, стараются вести непрерывный разговор с ней вплоть до получения денег. После чего сообщают, где можно увидеть своего родственника или знакомого.

Что делать в такой ситуации.

В первую очередь необходимо прекратить разговор и позвонить тому человеку, о ком идет речь. Если дозвониться ему не удалось, нужно постараться связаться с другими людьми, которым может быть известно его местонахождение (коллеги, друзья, родственники) для уточнения информации. Вероятнее всего на данном этапе Вы можете убедиться в том, что вас пытаются обмануть.

Несмотря на волнение за родственника или близкого человека нужно понимать, если незнакомый человек звонит Вам и требует привезти на некий адрес деньги – это мошенник. Если вы разговариваете якобы с сотрудником полиции, уточните, из какого он отделения. После чего позвоните в дежурную часть данного отделения и поинтересуйтесь, действительно ли ваш родственник или знакомый доставлялся туда.

Вместе с тем обращаем ваше внимание на то, что требование и передача взятки являются преступлениями.

SMS – сообщение с просьбой о помощи

Данный вид мошенничества – это упрощенная схема обмана по телефону, которому чаще всего поддаются пожилые и юные владельцы телефонов.

Как это работает:

Вам приходит на мобильный телефон сообщение: «У меня проблемы, переведи 3000 рублей на этот номер пожалуйста. Позже позвоню сам».

Как вести себя в подобной ситуации:

Пожилым людям, детям, подросткам необходимо объяснить, что на SMS-сообщения с незнакомых номеров реагировать категорически нельзя, так как чаще всего это мошенники!

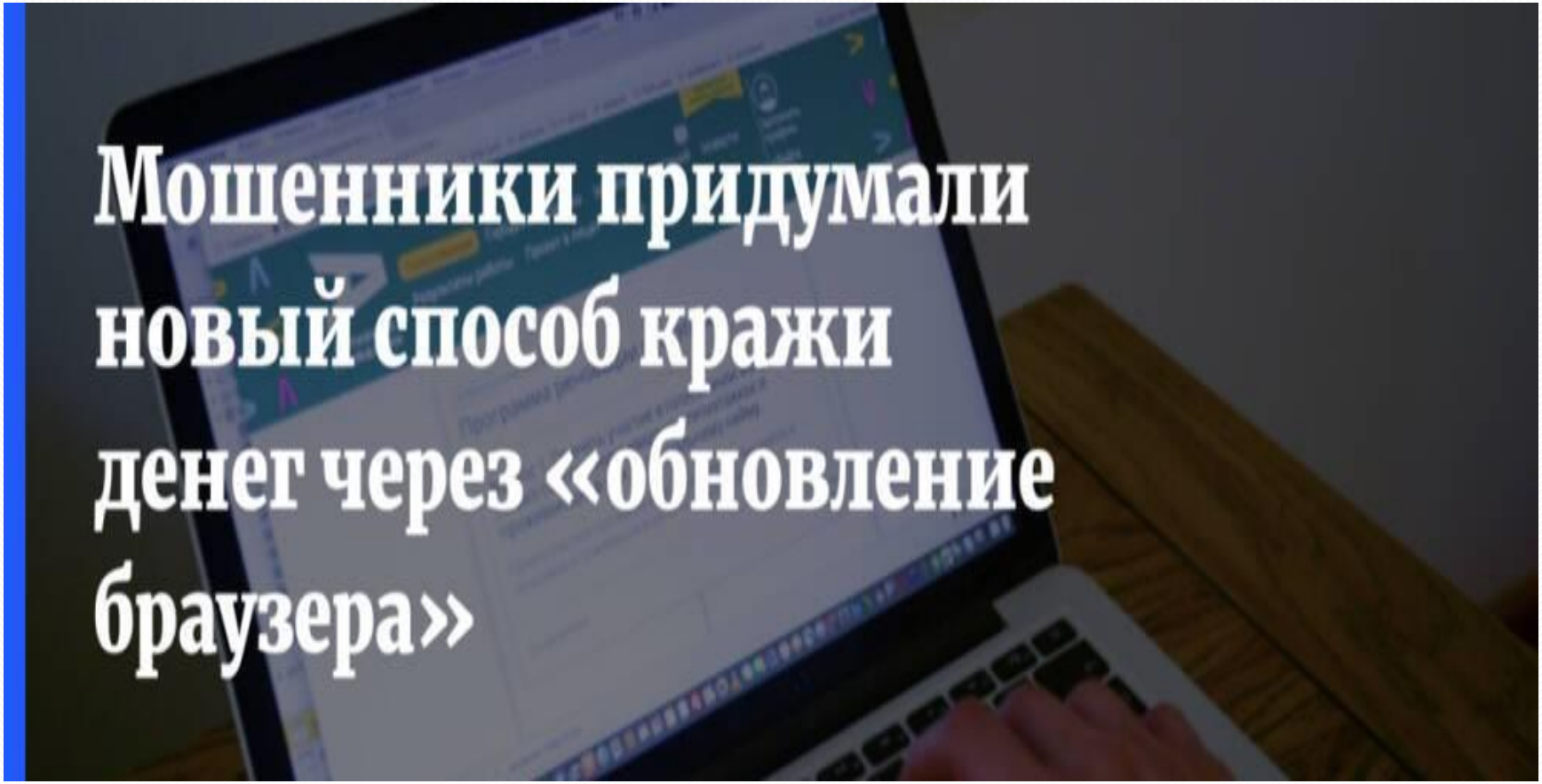
Телефонные вирусы

Очень часто злоумышленники пользуется телефонными вирусами. На ваш телефон приходит sms – сообщение следующего вида: «вам пришло mms – сообщение. Для получения пройдите по ссылке: htr...//», при переходе на которую, на телефон скачивается программа – вирус и происходит снятие денег с вашего счета, а также копирование информации, находящейся в вашем устройстве.

Что делать в подобной ситуации!

Не следует звонить по номеру телефона, с которого отправлено такое SMS-сообщение, особенно, если это короткий номер, состоящий из 3-6 цифр, вполне возможно, что в этом случае с вашего телефона будут автоматически сняты деньги.

Мошенники научились красть деньги через «обновление браузера»



Вредоносные мошеннические программы теперь могут проникнуть в телефон владельца через фиктивное обновление браузера. Это стало одной из актуальных схем обмана на смартфонах Android.

Так, при заходе на сайты онлайн-магазинов в браузере может появиться баннер (уведомление) о том, что текущая версия браузера устарела и необходимо обновить его для повышения уровня безопасности. При этом на баннере при внимательном прочтении можно заметить ошибки – например, может быть указана неверно текущая версия браузера.

Если нажать на обновление через такой баннер, то в смартфон будет скачано фиктивное обновление через фишинговый сайт, где пользователь введет свои настоящие данные и таким образом передаст их мошенникам.

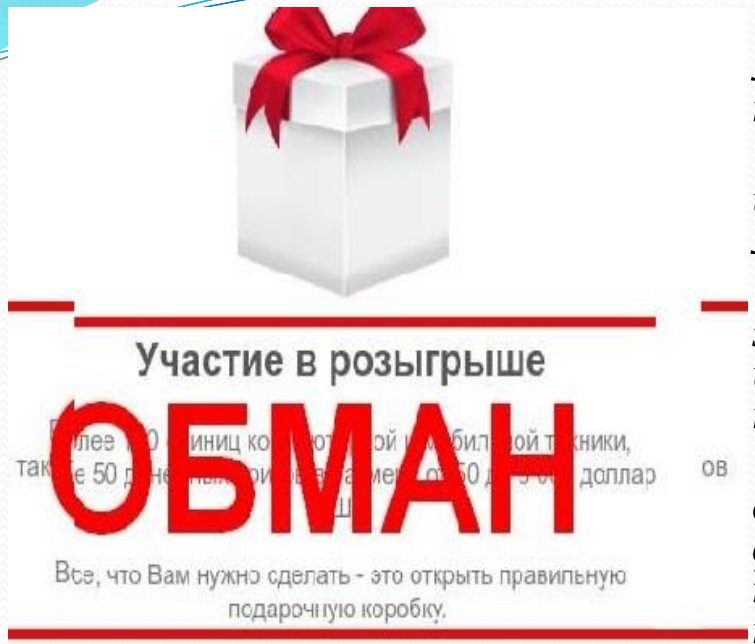
Так же в этот момент может быть скачан документ с вредоносным программным обеспечением.

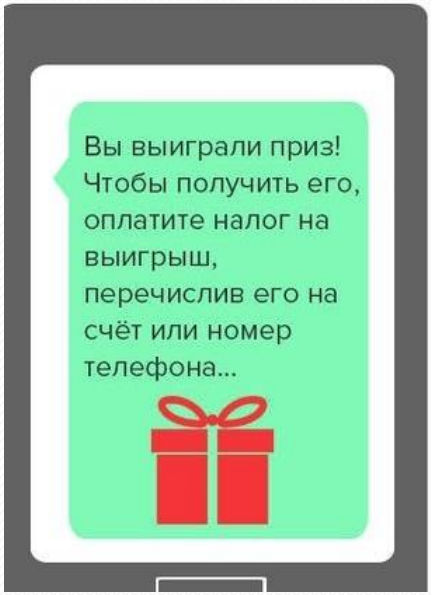
Возникновение аналогичных инцидентов не исключено и среди других операционных систем.

Наиболее популярные схемы мошенничества через интернет часто включают именно фишинговые сайты и скачивание «левых» приложений или документов, заражающих смартфон или планшет.

Например, сейчас активнее всего злоумышленники используют тему санкций, наложенных на российские банки и, как следствие, безопасности денег, которые хранятся в этих банках.

Розыгрыш призов





Одним из видов телефонного мошенничества является розыгрыш призов (это могут быть телефон, ноутбук, автомобиль и др.).

На ваш телефон приходит смс – сообщение, из которого следует, что в результате проведенной лотереи вы выиграли автомобиль.

Для уточнения всех деталей потенциальной жертве предлагается посетить определенный сайт и ознакомиться с условиями акции либо позвонить по одному из указанных телефонов.

Во время разговора по телефону мошенники сообщают о том, что для выполнения необходимых формальностей (уплата госпошлины, оформление необходимых документов, оплаты за комиссию перевода) счастливому обладателю новенького автомобиля (телефона, ноутбука) необходимо перечислить на счет указанную ими сумму, а затем набрать определенную комбинацию из 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 или какой либо иной приз, если вы не заполняли заявку на участие в ней либо каким-либо другим способом не подтверждали свое участи в розыгрыше, то вас пытаются обмануть. Будьте осторожны!

Мошенничество с банковскими картами

Одно из самых распространенных бесконтактных хищений происходит под предлогом попытки несанкционированного списания денег с вашей банковской карты.

Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча во время операций с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение.

Основные приемы, которые используют злоумышленники:

***скимминг** – или установка специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте;*

***траппинг** – установка на банкомат устройства, которое блокирует карту и не выдает ее обратно, а «добрый прохожий», якобы пытающийся помочь, подглядывает пин – код и после вашего ухода, забирает карту из банкомата и снимает с нее деньги;*

***фишинг** – рассылка электронных писем, в которых от имени банка сообщается об изменениях, производимых в системе его безопасности, при этом пользователей просят возобновить информацию о карте, в том числе указать ее номер и пин – код.*

Банковская карта – это пластиковая карта для совершения платежей и доступа к средствам, хранящимся на счете. За счет простоты использования банковских карт, у мошенников появляется множество способов для обмана.

Например, вам приходит sms – сообщение или поступает телефонный звонок от человека, который представляется сотрудником банка и сообщает, что ваша банковская карта заблокирована или кто-то пытается оплатить вашей картой товар или услуги.

И для получения подробной информации необходимо перезвонить на указанный номер и подтвердить данные вашей карты. Для снятия денег с вашей карты мошенникам нужен лишь ее номер и трехзначный код на обороте. Как только вы их сообщите, деньги будут сняты с вашего счета.

Помните!

Банковская карта является ключом к вашему счету. Поэтому никому ее не передавайте. Никогда не называйте реквизиты своей карты! Сотрудники банков никогда по телефону или в электронном виде не запрашивают персональные данные, реквизиты и срок действия карты. Они и так владеют информацией по вашей карте! В случае поступления информации о сомнительных операциях, обращайтесь непосредственно в банк или по телефону горячей линии, указанной на оборотной стороне карты.


Мошенники стали красть
деньги под предлогом
защиты от санкций

Мошенники придумали новую схему обмана на фоне введения санкций против российских банков.

Не секрет, что мошенники всегда умело использовали политическую и экономическую обстановку в стране и в мире для изобретения новых видов обмана.

Они начали звонить гражданам и требовать срочно снять все деньги со счетов в банке, потому, что они якобы скоро станут недоступны из-за отключения России от международной финансовой системы SWIFT и перевести их на «безопасные счета». Конечно же, это неправда. Если вам позвонили и начали уговаривать обезопасить свои средства или запугивать – вешайте трубку.

Для получения информации о своих вкладах и счетах пользуйтесь официальными сайтами.

Второй мошеннический способ, созданный на фоне политической ситуации, это фальшивые сборы на гуманитарную помощь. Таким образом, мошенники не только умеют выманивать деньги, но и делать за счет доверчивых граждан рекламу.

Общие рекомендации владельцам банковских карт

Чтобы не стать жертвой мошенников, необходимо соблюдать ряд следующих правил безопасности:

1. Никогда и никому не сообщайте ПИН- код вашей карты;

2. Нельзя хранить ПИН – код рядом с картой и тем более записывать ПИН – код на ней;

3. Пользуйтесь теми банкоматами, которые расположены в безопасных местах, оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках и крупных торговых центрах;

4. Обращайте внимание на картоприемник и клавиатуру банкомата, если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться;

5. В случае некорректной работы банкомата, если он самопроизвольно перезагружается – откажитесь от его использования;

6. Набирая ПИН – код, прикрывайте клавиатуру рукой;

Чтобы не стать жертвой мошенников, необходимо соблюдать ряд следующих правил безопасности:

7. *Не позволяйте никому использовать вашу пластиковую карту – это все равно, что отдать свой кошелек;*
8. *Никогда не прибегайте к помощи либо советам посторонних людей при проведении операций с банковской картой в банкоматах. Свяжитесь со службой поддержкой вашего банка – они обязаны проконсультировать вас по всем интересующим вопросам;*
9. *В магазинах, ресторанах, кафе все действия с вашей картой при оплате должны происходить только в вашем присутствии, в противном случае, мошенники могут получить данные вашей карты при помощи специальных устройств;*
10. *Если вы потеряли карту, срочно свяжитесь с банком, выдавшим ее, по телефону горячей линии, указанном на оборотной стороне карты, сообщите о случившемся и следуйте инструкциям сотрудника банка.*

Как уберечься от телефонных мошенничеств?

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

1) 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;

2) не следует отвечать на звонки или sms – сообщения с неизвестных номеров с просьбой положить на счет деньги;

3) 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.

Если вы стали жертвой мошенников обращайтесь по телефону 112 или 102 (02).