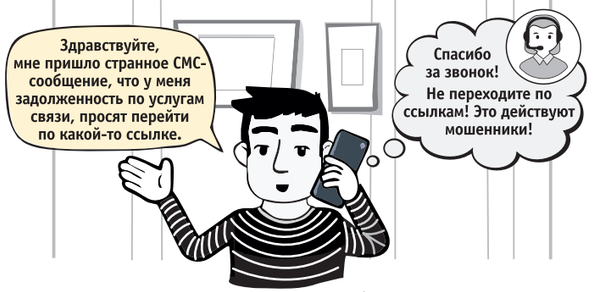
УМВД России «Пушкинское» информирует!

КАК ПРОТИВОСТОЯТЬ ТЕЛЕФОННЫМ МОШЕННИКАМ

- **НЕ ОТВЕЧАЙТЕ** на звонки с незнакомых номеров
- **ПРЕРВИТЕ РАЗГОВОР,** если он касается финансовых вопросов
- **НЕ ТОРОПИТЕСЬ** принимать решение
- **ПРОВЕРЬТЕ ИНФОРМАЦИЮ** в Интернете или обратитесь за помощью к близким родственникам
- **САМОСТОЯТЕЛЬНО ПОЗВОНИТЕ** близкому человеку / в банк / в организацию
- **НЕ ПЕРЕЗВАНИВАЙТЕ** на незнакомый Вам номер
- **ПРИНИМАЯ ФИНАНСОВОЕ РЕШЕНИЕ, ВОЗЬМИТЕ ПАУЗУ** и спросите совета у родных и друзей!
- **НЕ ПЕРЕДАВАЙТЕ** денежные средства и свои персональные данные незнакомым лицам

Звоните в полицию 02/102 или в дежурную часть УМВД России «Пушкинское» 8 (812) 573 18 90

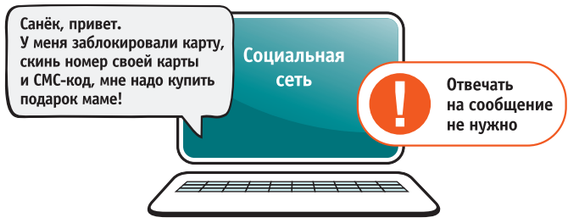
Электронные письма сомнительного характера



Ошибочный перевод средств

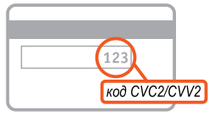
Сайт-дублер

«Друг» в соцсетях



При работе с сервисом «Интернет-Банк» Запсибкомбанка

Полезная информация:



- Для входа в Интернет-Банк необходимо ввести только логин и пароль, система никогда не запрашивает для входа: номер телефона, ПИН-код карты, код cvc2/cvv2.
- Если вы увидите на странице для входа в Интернет-Банк подозрительное с точки зрения источника сообщение – просьба немедленно обратиться в службу клиентской поддержки банка.
- Если вы забыли свой пароль, измените его в банкомате Запсибкомбанка или обратитесь в офис.

Как первый раз воспользоваться сервисом «Интернет-Банк»

1. Наберите в адресной строке: **https://inetbank.zapsibkombank.ru** или перейдите по соответствующей ссылке с сайта банка **www.zapsibkombank.ru**
2. Введите индивидуальный логин и пароль => Нажмите кнопку «Продолжить».

   Если вам подключил Интернет-Банк сотрудник банка, узнайте логин и пароль из полученного ПИН-конверта.

   Если вы подключили Интернет-Банк самостоятельно в банкомате, то введите логин, который был указан в чеке после подключения услуги, и пароль, который вы ввели в момент подключения сервиса.
3. На номер мобильного телефона, указанный вами при подключении сервиса «Интернет-Банк», придет СМС-сообщение с одноразовым паролем для подтверждения вашего входа в сервис.

   Если у вас нет возможности получить СМС-сообщение на данный номер, обратитесь лично к сотруднику Запсибкомбанка с паспортом.

   Введите одноразовый пароль, который получили в СМС-сообщении от Запсибкомбанка > Нажмите кнопку «Продолжить».

! Ни при каких обстоятельствах не сообщайте никому свои логин, пароль, а также пароль из СМС-сообщения.

4. Вход в Интернет-Банк совершен. В течение суток после подключения сервис может отображать не полную информацию по вашим банковским продуктам и сервисам.

! Если трудно запомнить свои логин и пароль, измените на более удобные в Интернет-Банке при первом входе в сервис > Раздел «Настройки». Пароль должен состоять из 4-х цифр, является конфиденциальной информацией и не подлежит разглашению.

При любых подозрениях, что открытый веб-сайт является мошенническим, имитирующим Интернет-Банк Запсибкомбанка, при подозрении в получении мошеннических СМС-сообщений или телефонных звонков, в которых неизвестные лица представляются как работники банка, убедительно просим вас обратиться в круглосуточную службу поддержки клиентов Запсибкомбанка или по номеру, указанному на обратной стороне банковской карты ПАО «Запсибкомбанк», либо по номеру, указанному на сайте банка **www.zapsibkombank.ru.**

При использовании банковских карт Запсибкомбанка

Полезная информация:

- Карта действительна до последнего дня месяца, указанного на ее лицевой стороне (напр.: 12/20 означает, что карта действительна до последнего дня декабря 2020 года).
- Изначально все карты, кроме карт Maestro, заблокированы от возможности расчетов в сети Интернет, кроме расчетов на тех сайтах, которые поддерживают технологию 3D-Secure. Для покупок на сайтах, не поддерживающих технологию 3D-Secure, необходимо активировать карту для расчетов на одну или несколько операций с помощью сервиса «Мобильный банк»/«Интернет-Банк». После совершения покупки вы можете обратно заблокировать карту от расчетов в сети Интернет с помощью сервиса «Мобильный Банк» или «Интернет-Банк».
- В случае утраты карты необходимо немедленно позвонить в круглосуточную службу поддержки клиентов банка или отправить соответствующее СМС-сообщение с помощью «Мобильного Банка», «Интернет-Банка» или его мобильного приложения для блокирования карты.
- По картам установлены лимиты на выдачу наличных. Ознакомиться с лимитами на выдачу наличных вы можете на сайте банка www.zapsibkombank.ru, в Интернет-Банке в разделе «Счета и карты», а также в офисе банка.

Общие рекомендации для обеспечения безопасности

1. Убедитесь, что для входа в Интернет-Банк требуется ввести только логин, пароль и одноразовый пароль на вход из СМС-сообщения.
2. Проверяйте адрес Интернет-Банка https://inetbank.zapsibkombank.ru. Если вы видите другой адрес, то сообщите об этом в банк.
3. Ни в коем случае не вводите свои логин и пароль в представленную на неопознанном сайте форму.
4. Убедитесь, что адресная строка начинается с https:// (установлено защищенное соединение с сервером банка).
5. В адресной строке вашего веб-браузера должен быть изображен значок закрытого замка.
6. Для ввода пароля безопаснее пользоваться виртуальной экранной клавиатурой, особенно когда пользуетесь чужим компьютером.
7. Пользуйтесь современным антивирусным решением, по возможности – с функцией защиты от интернет-мошенничества.
8. Регулярно обновляйте операционную систему, антивирусное программное обеспечение и веб-браузер.
9. Внимательно просматривайте выписки о ваших операциях в Интернет-Банке. После завершения работы в Интернет-Банке пользуйтесь кнопкой «Выход».

Официальные банковские ресурсы

Официальный сайт ПАО «Запсибкомбанк»: www.zapsibkombank.ru

Адреса интернет-банков:

Для физических лиц «Интернет-Банк» https://inetbank.zapsibkombank.ru/

Для юридических лиц «ЗапСиб iNet» https://www.zapsibkombank.ru/corporate/inet/

Просим проявлять бдительность и осторожность!

Группа ВТБ

Памятка по защите от мошеннических действий

- **При соблюдении правил безопасности ваши финансы будут под надежной защитой**

Контактная информация

Единая справочная служба Запсибкомбанка

8-800-100-5005 (звонок по РФ бесплатно)

Запсибкомбанк

Главное - быть полезным

ПАО «Запсибкомбанк», Ген. лицензия ЦБ РФ №918 от 13.07.2015 г.

Осторожно! Мошенничество по мобильному телефону!

- **Звонок от сотрудника «службы безопасности банка», «центра финансовой безопасности» и т.п. служб.** Поступает звонок об одобрении кредита, возврате страховки, о совершении подозрительного перевода. Просят назвать коды из СМС-сообщений непосредственно во время разговора либо переключают на голосового помощника, либо просят подойти к банкомату для совершения определенных действий.
- **Звонок от покупателя.** По размещенному объявлению о продаже поступает звонок от покупателя, который просит сообщить данные карты (логин/пароль, ПИН-коды, CVC2/CVV2 (последние 3 цифры на обратной стороне карты)) для перевода оплаты.
- **Просьба о помощи.** СМС-сообщение или пост в мессенджерах. Мошенники под видом близких родственников: «мамы», «друга», «сына» просят перевести определенную сумму на указанный номер.
- **Телефонный номер-грабитель.** Сообщение с незнакомого номера с просьбой перезвонить по любой причине – проблема со связью, смена тарифа, помощь другу и т.д. В случае обратного звонка с вашего счета спишется денежная сумма.
- **Ошибочный перевод средств.** Приходит СМС-сообщение о якобы поступивших средствах на счет. После этого поступает звонок или еще одно СМС-сообщение с просьбой вернуть деньги обратно, т.к. они отправлены по ошибке не на тот номер.
- **Требование выкупа.** Звонок с требованием выкупа или взятки за освобождение якобы из отделения полиции знакомого или родственника.

Правила безопасности

- **При звонке из «службы безопасности банка» или «центра финансовой безопасности» и т.п. служб ответьте, что перезвоните сами и положите трубку. Совершите звонок в банк по номеру телефона, указанному на обратной стороне банковской карты.**
- В случае каких-либо сомнений – не перезванивать по указанным номерам, не отправлять ответных СМС-сообщений, не переводить средства на незнакомые номера, никому не сообщать логин/пароль, ПИН-коды, CVC2/CVV2 (последние 3 цифры на обратной стороне карты), или другие коды, которые приходят, срок действия карты.
- Важно помнить, что нельзя вводить свой номер телефона на незнакомых сайтах для регистрации или подтверждения какой-либо информации, а также устанавливать на телефоны приложения из неофициальных источников, не рекомендованных производителем мобильного телефона.
- Всегда связываться напрямую с близким или родственником, банком, оператором связи и т.д.
- Подключите сервис «Мобильный банк» или оповещение на адрес электронной почты для информирования о проводимых операциях.
- Будьте бдительными и помните о существовании мошеннических схем!

Осторожно! Мошенничество в сети Интернет!

- **«Друг» в социальных сетях** просит помощи или оплатить товар. Как правило, просят прислать номер вашей карты и код подтверждения операции.
- **Сайт-дублёр** – это сайт, который внешне повторяет настоящий сайт организации и имеет похожее написание имени сайта в адресной строке браузера.
- **Вредоносные программы** заражают смартфон или компьютер. При переводе денежных средств вирус показывает так называемые «веб-фейки» – окна браузера, визуально схожие с окнами авторизации банковских операций. При вводе в них данных банковских карт денежные средства отправляются злоумышленникам.
- **Электронные письма сомнительного характера.** Это могут быть письма с несуществующими вакансиями, просьбы отправить взнос за какие-либо дополнительные услуги, письма с назначением встречи в онлайн-календаре, письма-угрозы, в которых мошенники шантажируют, требуя перевести им денежные средства взамен конфиденциальной информации о вас.
- **Фишинг** – письма с предложением товаров, поддельные письма от представителей официальных организаций или банков. В сообщении просят предпринять незамедлительные действия, затрагивающие ваш аккаунт, например, подтвердить детали банковского счета, изменить пароль, получить приз. Может использоваться текущая ситуация (стихийные бедствия, финансовые проблемы, праздничные мероприятия), чтобы заставить перейти по ссылке или открыть вложение. Большинство фишинговых писем содержат ссылки на поддельные веб-сайты, с помощью которых похищаются конфиденциальные данные (логины, пароли, номера карт и т.д.), либо выполняется операция по перечислению денежных средств на счета злоумышленников.

Правила безопасного использования сети Интернет

- Быть бдительными и внимательными при получении сообщений или писем, в которых вас просят выполнить переводы средств или покупку чего-либо.
- Перепроверяйте любую полученную информацию.
- Не открывайте файлы-вложения от неизвестных отправителей.
- По возможности не сохраняйте в системе пароли и периодически меняйте их.
- Не переходите по гиперссылкам в письме.

При совершении операций через Интернет

- Не используйте ПИН-код при заказе товаров и услуг в Интернет, а также по телефону/факсу.
- Пользуйтесь Интернет-сайтами только известных и проверенных организаций торговли и услуг.
- Обязательно убедитесь в правильности адресов Интернет-сайтов, на которых собираетесь совершить покупки.
- По возможности совершайте покупки только со своего компьютера.
- Установите на свой компьютер антивирусное программное обеспечение и регулярно производите его обновление.

Осторожно! Мошенничество с банковскими картами!

- **«Ваша карта заблокирована!», «Совершен платеж».** Подобные СМС-сообщения приходят с неизвестных номеров. При звонке на указанный номер вас просят сообщить номер банковской карты, CVC2/CVV2 или ПИН-код.
- **Карта попала в чужие руки.** Любой продавец в магазине, кафе, на заправке может сфотографировать, переписать данные банковской карты или просто запомнить и передать мошенникам для изготовления дубликата карты.
- **Оплата дважды.** При расчете за покупку кассир сообщает об ошибке и просит повторно произвести оплату. Спустя какое-то время вы обнаруживаете, что деньги за покупку были списаны дважды.
- **Близнецы-«симки».** Этот способ используется, когда мошенники уже завладели данными карты и им необходимо при помощи кода из СМС-сообщения подтвердить транзакцию перевода денег на нужный счет. С помощью дубликата мошенники получают полный контроль над счетами, так как банковские карты, как правило, могут управляться дистанционно с телефона.

Правила безопасного использования банковских карт

При оплате товаров и услуг

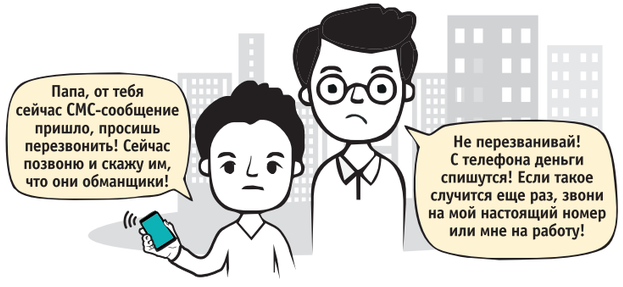
- Не выпускайте из поле зрения карту – все операции с картой должны проводиться на ваших глазах. Перед набором ПИН-кода следует убедиться в том, что люди, находящиеся в непосредственной близости, не смогут его увидеть.
- Кассир может потребовать предоставить паспорт, подписать чек или ввести ПИН-код. Перед тем как подписать чек, нужно в обязательном порядке проверить, чтобы сумма, снятая с карты, соответствовала сумме купленных товаров.
- Если при попытке оплаты банковской картой произошла «неуспешная» операция, следует сохранить один экземпляр выданного терминалом чека для последующей проверки на отсутствие указанной операции в выписке по банковскому счету.
- В случае любых сомнений безопасности использования карты лучше обратиться в банк с заявлением о ее перевыпуске.
- Установите индивидуальный расходный лимит по карте с бесконтактным платежом и ограничьте количество возможных транзакций.

При совершении операций в банкомате/инфокиоске

- Перед использованием устройства осмотрите его на наличие мошеннических устройств (накладок), расположенных в месте набора ПИН-кода и в месте, предназначенном для приема карт (прорезь). Если что-то покажется подозрительным, не используйте устройство. Сообщите о ваших подозрениях в службу поддержки банка, указав адрес расположения устройства, которое вызвало у вас подозрение.
- Набирайте ПИН-код так, чтобы стоящие рядом люди не могли его увидеть. Прикрывайте клавиатуру рукой.
- Запрещается ввод ПИН-кода в пропускные устройства для доступа в помещение, где расположен банкомат/инфокиоск.
- В случае захвата карты устройством необходимо заблокировать карту по телефону, указанному на сайте банка или через сервис «Интернет-Банк» или его мобильное приложение.
- В момент получения денег не отвлекайтесь на сторонние разговоры и звонки. Дождитесь выдачи денег, заберите и пересчитайте их.
- Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций с банковской картой в банкоматах/инфокиосках.

СМС-сообщения с просьбой о помощи

Телефонный номер-грабитель



Выигрыш в лотерее

«Ваша карта заблокирована!»

ОСТОРОЖНО, МОШЕННИКИ!

ПРОКУРАТУРА САНКТ-ПЕТЕРБУРГА ПРЕДУПРЕЖДАЕТ

ОСНОВНЫЕ ПРИЗНАКИ ОБМАНА ВО ВРЕМЯ КОНТАКТА С МОШЕННИКАМИ:

1. ПРЕДСТАВЛЕНИЕ СОТРУДНИКАМИ ПРАВООХРАНИТЕЛЬНЫХ И ГОСУДАРСТВЕННЫХ ОРГАНОВ, ЦЕНТРАЛЬНОГО БАНКА РОССИИ, ПУБЛИЧНЫХ ОРГАНИЗАЦИЙ

2. УВЕРЕННАЯ И УВАЖИТЕЛЬНАЯ МАНЕРА ОБЩЕНИЯ, ИСКЛЮЧАЮЩАЯ ВОЗМОЖНОСТЬ УСОМНИТЬСЯ В КОМПЕТЕНТНОСТИ

3. СООБЩЕНИЕ О ФАКТАХ, ПРЕДСТАВЛЯЮЩИХ КАКУЮ-ЛИБО УГРОЗУ

4. ПРЕДЛОЖЕНИЕ УДАЛЕННО РЕШИТЬ ПРОБЛЕМУ, СООБЩИВ КОД ИЗ СМС, РЕКВИЗИТЫ БАНКОВСКОЙ КАРТЫ ИЛИ ДРУГИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5. ОБЕЩАНИЕ ВЫСОКОГО ДОХОДА, УВЕЛИЧЕНИЯ ПЕНСИИ, ПОЛУЧЕНИЯ ПОДАРКОВ

6. ПРИЗЫВ К НЕМЕДЛЕННЫМ ДЕЙСТВИЯМ, ИСКЛЮЧАЮЩИЙ ПРИНЯТИЕ ВЗВЕШАННОГО РЕШЕНИЯ

КАК ИЗБЕЖАТЬ ОБМАНА:

1. СБРАСЫВАЙТЕ ЗВОНКИ НЕЗНАКОМЦЕВ!

2. ПОМНИТЕ – НАСТОЯЩИЕ ГОСУДАРСТВЕННЫЕ СЛУЖАЩИЕ, РАБОТНИКИ БАНКОВ И ПУБЛИЧНЫХ ОРГАНИЗАЦИЙ НЕ ИНФОРМИРУЮТ ГРАЖДАН ОБ УГРОЗАХ ПО ТЕЛЕФОНУ ИЛИ ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ!

3. ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ ДО ПРИНЯТИЯ РЕШЕНИЯ!

4. СОВЕТУЙТЕСЬ С ТЕМИ, КОМУ ДОВЕРЯЕТЕ!

БУДЬТЕ В КУРСЕ, УЗНАВАЙТЕ СХЕМЫ МОШЕННИЧЕСТВА И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

«Почему нет воды и когда появиться?» - один из самых популярных запросов в сезон отключения воды - с мая по август. Как аферисты ловят жертву на живца?

Мошенники рассылают фейковые письма с предложением проверить график отключения горячей воды. Цель остается той же - похитить персональные данные. Ссылки в таких письмах ведут на фишинговые сайты, с помощью которых злоумышленники получают доступ к персональной информации.

Уважаемые петербуржцы! Проверяйте график отключений только на официальных ресурсах:

- на сайтах и в соцсетях управляющих компаний и местных администраций;

- на информационных стендах внутри подъездов и на входных группах;

- на "Госуслугах".

Как работает схема?

Аферисты выдают себя за работников образовательной организации. Они требуют школьника подтвердить номер телефона якобы для электронного журнала. Вместо номера ребенку направляют код авторизации от портала «Госуслуги». После мошенническая атака может продолжиться по по схеме "фейк босс".

Школьнику могут звонить из Следственного Комитета, Центрального Банка и других организаций. Мошенники требуют провести обыск в квартире и показать, где лежат ценности. В стрессовой ситуации, школьник соглашается провести «видеообыск» и «задекларировать» ценности. Далее ценности передают курьеру.

Кто может стать жертвой?

Схема нацелена на подростков. Кем представиться злоумышленники выбирают, как правило, из числа педагогов, которые недавно работают в организации. Они создают фейковые аккаунты, маскируясь под директоров, завучей, учителей школ или вузов (указывают соответствующие личные данные, копируют фото реального профиля и т. п.) и начинают от их лица звонить жертве.

Как уберечь себя от мошенников?

Будьте максимально критичны, проверяйте информацию, никому не сообщайте коды по телефону. Атаки мошенников, направленные на детей и подростков, фиксируются регулярно, поэтому призываем поговорить с детьми о киберугрозах, рассказать о новой схеме.

Информационная справка

За 7 месяцев 2025 года количество пострадавших на территории Пушкинского района от действий мошенников составило не менее 400 граждан.

Согласно проведенным экспертизам установлено, что злоумышленники, представляясь сотрудниками правоохранительных органов, Центрального банка России, оказывают на потерпевших массированное психологическое воздействие, удерживают их в состоянии постоянного напряжения и страха, манипулируют и запугивают их. Используемые злоумышленниками программы и сервисы администрируются из-за рубежа, в связи с чем организаторы зачастую недоступны для правоохранительных органов России, а поручения об оказании международно-правовой помощи в западные страны остаются без ответа. Вместе с тем, нами устанавливаются исполнители, действующие на территории г. Санкт-Петербурга и России, однако, их привлечение к уголовной ответственности является недостаточным для прекращения преступлений данной категории.

Самыми распространенными способами совершения преступлений являются:

- **осуществление телефонного звонка от имени любого должностного лица правоохранительных органов** (МВД, ФСБ, прокуратуры), Центрального банка России, службы безопасности конкретного банка. В ходе разговора мошенники, зная ФИО потерпевшего и наличие у него банковского счета в конкретном банке, то есть обладая персональными данными потерпевшего, сообщают ему о попытке хищения денежных средств с его счета, чем вводят его в тревогу относительно утраты нажитого имущества. При этом, оказывая психологическое воздействие, сообщают единственный выход из сложившейся ситуации - перевести деньги на «безопасный государственный счет» на период установления и задержания виновного лица, после чего убеждают потерпевшего снять деньги со своего счета и зачислить их в банкомате на продиктованный счет. В подтверждение своих слов о причастности к государственным органам, преступники демонстрируют потерпевшему с помощью различных мессенджеров документы государственных органов или служебные удостоверения, которые в действительности являются фиктивными. Аналогичным способом преступники убеждают потерпевших оформить на свое имя кредит, денежные средства перевести на «безопасный счет», после чего они похищаются.
- **представляясь сотрудниками МВД, либо ФСБ**, преступники обманывают граждан, сообщая им о наличии угрозы потери квартиры, убеждают их в том, что они участвуют в мероприятиях по поимке

мошенников путем продажи квартиры и временного помещения вырученных от продажи денег на «безопасный счет», которые на самом деле похищаются.

- **хищение денег граждан путем совершения звонка от имени близкого родственника или знакомого**, якобы попавшего в беду (совершившего дорожно-транспортное происшествие или иное преступление), с требованием передачи денежных средств для избежания уголовной ответственности, которые в последующем преступники похищают через подставных лиц (таксистов, курьеров), как правило не осведомленных о совершаемом преступлении.
- «**удаленная работа, дополнительный быстрый заработок**». Потерпевший, желая получить «легкие деньги» вступает в групповые чаты, в которых предлагается, например, осуществлять бронирование номеров в гостиницах и предоставлять скриншоты об оплате, осуществлять покупку/продажу товаров, «раскручивать» аккаунты социальных сетей, для данных целей мошенники предоставляют жертвам банковские реквизиты для перевода либо ссылки на фишинговые сайты, при этом создавая активность таких чатов с помощью ботов и видимость, что другие участники тоже совершают покупки и получают прибыль. При этом поначалу потерпевшие получают якобы «прибыль», тем самым мошенники усыпляют бдительность и убеждают потерпевших вкладывать и выбирать задания более высокого уровня на крупную сумму, но когда суммы покупок/оплаты достигают значительных размеров, то мошенники, завладев денежными средствами жертв, удаляют чаты и переписки, меняют абонентские номера.
- **«запись на диспансеризацию, установка приложения для записи к врачам, программы-вирусы»**. Мошенники обзванивают потерпевших, представляются сотрудниками медицинских учреждений, приглашают пройти диспансеризацию, на которую возможно записаться по телефону, необходимо лишь для подтверждения записи к врачам сообщить код из смс, с помощью которого получают доступ к Госуслугам, где мошенники получают массу персональной информации, которую в последующем могут использовать в других мошеннических схемах. В случае программ – вирусов потерпевшие теряют доступ к своему устройству и под угрозой оказываются все приложения с персональными и платежными данными, в том числе банковскими.
- **«Инвестиции»**. Существуют многочисленные способы вовлечения потерпевших в инвестирование: знакомство в социальных сетях, где поначалу идет отстраненная переписка мошенника с жертвой на общие темы, постепенно с переходом о вопросе дополнительного заработка и во влечении в «инвестирование»; различные рекламы и объявления в

сети Интернет о вложении в криптовалюту и гарантии невероятной прибыли от инвестиций. Далее мошенники в ходе общения в мессенджерах, в ряде случаев в действительности рассказывают основные принципы торговли, для того чтобы притупить бдительность жертвы. Человек, мечтая получить огромные доходы, начинает перечислять денежные средства на мифический инвестиционный фонд, зачастую жертвы даже не обращают внимания, что перечисляет денежные средства на банковские счета физических лиц – дропов. В последующем потерпевший не получает никакой прибыли, при этом ему сообщают о заблокированном счете и для того, чтобы вывести денежные средства необходимо разблокировать счет, путем перечисления денежных средств на определенный процент от «полученной прибыли», ради чего потерпевшие даже оформляют кредиты, перечисляя снова и снова денежные средства мошенникам.

- **взлом аккаунтов профиля социальных сетей мессенджеров** (ВКонтакте, WhatsApp, Telegram), так при получения доступа к персональным данным жертвы, мошенники рассылают сообщения неопределенному кругу лиц от имени потерпевшего в указанных сервисах, с просьбой «срочно одолжить денежные средства» путем их перевода на номера банковских карт указанные мошенниками, либо с предоставлением фотографии банковской карты, на которой указаны данные потерпевшего, однако номер банковской карты полностью подконтролен мошеннику.
- **«Вами выдана доверенность на Госуслугах на оформление кредитов, продажу квартиры, распоряжение счетами, срочно берите встречные кредиты для аннулирования кредитов, продавайте имущество и перечисляйте все денежные средства на «безопасный счет»»**. При данной схеме мошенники для убедительности предоставляют на электронную почту поддельные доверенности, в которых указано, что потерпевший якобы в действительности доверил некому гражданину оформление кредитов/продажу квартиры/машины, также присылают копии документов с логотипами Банка России, гербовые печати, документы сотрудников Банка и иных должностных лиц, при этом разговор жертвы и мошенника может длиться достаточно продолжительное время, а в некоторых случаях и до нескольких дней. Мошенники убеждают жертву оформить кредиты, снять все свои сбережения, закрыть вклады в банках и осуществить переводы денежных средств на «безопасные счета», уверяя, что после поимки преступника денежные средства/имущество в полном объеме вернутся потерпевшему. Мошенники убеждают потерпевшего не сообщать ничего родственникам, заказывают жертвам такси для перемещения от дома до банков, при этом указывая в какой именно банк обратиться за

кредитом либо осуществить снятие денежных средств в крупной сумме, указывают в каком именно банкомате осуществить внесения денежных средств на «безопасный счет». Некоторые потерпевшие, будучи под влиянием обмана, по указаниям мошенников перемещаются в другие города в тайне от родственников, не контактируя с родственниками некоторое время, отдают мошенникам все свои сбережения, вплоть до срочной продажи квартир и иной недвижимости с последующим перечислением вырученных денежных средств от сделки мошенникам.

- **«Фишинговые сайты, письма, сообщения»**. Фишинг — вид интернет-мошенничества, цель которого получить доступ к данным пользователя: логинам и паролям, номерам карт, банковским счетам. Преступники присылают фишинговые письма, которые могут быть очень похожи на настоящие сообщения от банков, компаний, органов власти или Госуслуг. Но ссылка в таком письме ведёт на поддельный сайт. Став жертвой фишинга, можно лишиться денег или доступа к своим учётным записям, пустить хакера в корпоративную сеть работодателя. Фишинговыми бывают не только письма, приходящие на электронную почту. Это могут быть сообщения в мессенджерах, социальных сетях и смс. Злоумышленники имитируют письма от администрации социальных сетей, интернет-магазинов. При переходе по ссылке вы окажетесь на сайте, который оформлен как настоящий интернет-сервис и при оплате например приобретаемого товара денежные средства зачисляются на счета мошенников.
- **«пролонгация абонентского договора с оператором сотовой связи/взлом Госуслуг»**. Схема заключается в том, что гражданину звонит якобы представитель сотового оператора, у которого обслуживается номер телефона гражданина. Мошенники говорят, что номер старый, обслуживается, например, больше десяти лет, и его необходимо "пролонгировать". Иначе номер будет передан новому абоненту и уверяют что возможно сделать это по телефону, без траты времени на посещения салона связи. В том числе Пролонгировать абонентский номер предлагается через сайт «Госуслуги». И всего лишь нужно продиктовать код из пришедшего сообщения, продиктовав код у мошенников появляется доступ к личному кабинету Госуслуг жертвы. И далее различные негативные последствия, самые нежелательные из которых - микрозаймы и кредиты на имя гражданина.
- **«продление Полиса ОСАГО»**. Мошенники рассылают письма на электронные почты, смс сообщения о заканчивающемся сроки полиса ОСАГО с ссылками на сайты для продления действия полиса. Как правило у жертвы в действительности подходит срок действия полиса. Так, потерпевший переходит на сайт якобы страховой компании – фишинговый сайт, где после заполнения некоторых полей, в том числе

реквизитов банковской карты, подтвердив операцию по оплате, деньги списываются, а на электронную почту приходит файл с полисом похожего на действительный, однако при его проверке в базе РСА такого полиса найдено не будет.

- **«покупка/продажа товаров на торговых площадках».** Мошенничество с помощью торговых площадок, на примере самой распространенной - Авито. Имеется несколько популярных видов мошенничеств:
  1) Вы — покупатель и нашли объявление о продаже товара, которое Вас заинтересовало. На ваше предложение купить товар продавец отвечает, что к нему уже выстраивается очередь из покупателей — и если вы точно хотите получить вещь, то должны отправить ему на карту предоплату. После продавец предоставляет реквизиты для перевода и завладев денежными средствами скрывается.
  2) Вы — продавец. «Покупатель - мошенник» готов купить ваш товар, не глядя, и хочет отправить вам на карту задаток или даже полностью оплатить вещь. Он просит номер карты, а затем требует назвать цифры из СМС, которое пришло вам из банка — якобы это нужно для банковского перевода.
  3) покупатель - мошенник спрашивает у вас номер карты, чтобы отправить вам деньги за товар при личной встрече, однако деньги на счет не поступают, в подтверждении своих добросовестных намерений покупатель - мошенник демонстрирует подложные квитанции о переводе, списание с его счета денег, сообщает свои данные паспорта и ФИО, но в большинстве случаев все эти данные фальсифицированы, также ссылаются на сбой работы банка и убеждают что денежные средства поступят возможно позже, так мошенник завладевает имуществом, не имея намерений производить оплату.
  4) Вы - покупатель. Продавец предлагает вам общаться не в собственном мессенджере «Авито», а в другом — например, в WhatsApp. Он находится в другом городе и готов отправить вам товар, но вместо сервиса «Авито Доставка» хочет воспользоваться сторонней курьерской службой доставки — Boxberry, «СДЭК» и другими. Продавец спрашивает ваши личные данные: ФИО, адрес и номер телефона - для отправки товара, но только в случае оплаты всей стоимости товара путем перевода на банковские реквизиты указанные мошенником. Затем злоумышленник предоставляет поддельную квитанцию и трек номер отправления транспортной компании, таким образом получив денежные средства путем обмана, не намереваясь отправлять товар. Также бывают случаи, когда присылают ссылку на курьерскую службу, и вы оплачиваете картой товар. Через некоторое время вам сообщат, что произошла

ошибка или внештатная ситуация, и вы не сможете получить свой товар. Вам предложат возврат средств — для этого снова придётся ввести данные карты на сайте курьерской службы. Под предлогом возврата средств мошенники ещё раз спишут деньги с вашей карты. Сайт и служба поддержки «курьерской компании» — поддельные. Ещё один вариант развития событий, это когда «Продавец» якобы готов отправить вам товар с помощью сервиса «Авито Доставка» и для удобства общения он предлагает вам перейти в сторонний мессенджер — WhatsApp или Telegram — и в нём присылает ссылку на форму «Авито Доставка», чтобы вы оплатили товар картой. И идентичная схема когда Вы — продавец, «Покупатель» готов купить у вас товар с помощью «Авито Доставки». В мессенджере «Авито» он спрашивает ваш адрес электронной почты — туда вам приходит письмо из сервиса «Авито Доставка». В письме содержится форма, где нужно указать данные вашей карты для получения денег от покупателя, однако сайт фишинговый и денежные средства похищает мошенник.

Типичные фразы мошенников:

- «Продиктуйте пароль из СМС»;
- «На вашу карту пришел крупный денежный перевод»;
- «Назовите данные банковской карты»;
- «На вашей карте замечена подозрительная активность»;
- «Ваша сим-карта была заблокирована»;
- «Это служба безопасности банка. С вашего счета списали деньги»;
- «Это сотрудник полиции. Переведите свои деньги на безопасный счет».

С целью избежания хищения денежных средств необходимо соблюдать ряд правил, а именно:

- Не разглашать персональные данные в ходе телефонного разговора;
- Не осуществлять предоплату по объявлениям с сайтов;
- Не сообщать любые данные банковских карт или код из СМС;
- Не переводить денежные средства незнакомым людям.

Рекомендуется:

- Не переходить по сторонним ссылкам, поступившим на мобильный телефон с помощью СМС сообщений или в мессенджерах;
- Быть внимательными. Не терять самообладание во время телефонного разговора;
- Прервать телефонный разговор с мошенниками;
- Связаться с родственниками, сообщить им о поступившем звонке, посоветоваться с ними;
- Заблокировать подозрительного абонента.