



МВД России

**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
ПО РЕСПУБЛИКЕ МАРИЙ ЭЛ
(МВД по Республике Марий Эл)**

ул. Комсомольская, 139, Йошкар-Ола, 424000

«*ИР*» февраля 2024 г. № 1/ *644*
на № _____ от _____

Руководителям министерств
и ведомств Республики
Марий Эл, территориальных
органов федеральных органов
исполнительной власти,
расположенных на территории
Республики Марий Эл,
главам администраций
муниципальных образований
Республики Марий Эл
(по списку)

О направлении информации

Уважаемые руководители!

В прошлом году на территории Республики Марий Эл сохранилась тенденция увеличения числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

В 2023 году регистрация таких преступлений выросла на 48,3% (с 2634 до 3919), их удельный вес в структуре преступности – с 34,0% до 47,2%.

Преступления данного вида в минувшем году зарегистрированы на территории всех муниципальных образований.

Количество потерпевших от дистанционных преступлений выросло более чем в полтора раза (+57,9%, 3092 гражданина, 2022 г.: 1958), из которых 730 пенсионеры (23,6%, 2022 г.: 429 или 21,9%).

Сумма материального ущерба по преступлениям данной категории составила 534,73 млн рублей (2022 г.: 325,1 млн рублей), из них возмещено только 5,37 млн рублей или 1,0%.

В связи с изложенным, особую актуальность приобретает профилактика киберпреступности, в том числе повышение осведомленности граждан о способах их совершения и методах защиты от них.

Проведенная в минувшем году информационно-пропагандистская и профилактическая работа с населением способствовала росту в два раза количества дистанционных мошенничеств, пресеченных на стадии покушения (+92,3%, с 271 до 521), их доля возросла почти на десять процентов и составила 28,4% (2022 г.: 20,6%).

В текущем году криминальная активность киберпреступников не снижается, уже зарегистрировано 825 дистанционных хищений (аналогичный период прошлого года: 549; +50,3%).

В целях профилактики дистанционных хищений направляю Вам сведения об основных схемах, используемых преступниками в настоящее время для хищений денежных средств граждан и способах защиты от них, а также памятку по профилактике мошенничеств.

Также информирую, что профилактические аудио- и видеоролик «Осторожно мошенники!», которые размещены и доступны для скачивания на официальном сайте МВД по Республике Марий Эл в сети Интернет¹.

Прошу довести указанную информацию до сотрудников и работников Ваших министерств и ведомств, подведомственных учреждений, а также использовать при работе с населением и разместить на собственных сайтах.

Приложение: по тексту, на 6 л. в 1 экз.

Министр



А.В. Вырвич

¹ Адрес: <https://12.мвд.рф/> «ПРЕСС-СЛУЖБА»/«Наши проекты» / «ОСТОРОЖНО, МОШЕННИКИ!»/ «Социальные видеоролики».

Основные схемы мошенничеств

1. Звонок от службы безопасности банка либо сотрудников полиции или ФСБ «Неизвестные пытаются оформить на ваше имя кредит», а также другие мошенничества с банковскими картами.

В феврале 2024 года 66-летнего йошкар-олинца аферисты обманули, используя стандартную схему, которая начиналась со звонка от якобы «сотрудника ФСБ» с сообщением, что неизвестными совершена попытка оформления кредита на его имя. Предложив пресечь хищение, потерпевшего убедили оформить встречный кредит на как можно большую сумму, а затем снять деньги и перечислить их на «безопасный счет». Мошенник объяснил это тем, что требуется исчерпать «кредитный лимит». В итоге местный житель, следуя рекомендации афериста, оформив кредит на сумму более двух с половиной миллиона рублей, перевел его на указанные мошенником счета через банкоматы в крупном торговом центре города.

Меры противодействия: Звонок из банка под предлогом предотвращения несанкционированного списания денежных средств или нелегального оформления кредита – стандартная уловка злоумышленников. При поступлении подобного звонка необходимо сразу же прекратить диалог и набрать номер телефона, который размещен на банковской карте. Ни в коем случае не передавайте незнакомцам CVV-код с обратной стороны карты и пароли доступа, которые приходят в смс-уведомлениях, не устанавливайте по совету собеседников на компьютеры и смартфоны программы, не выполняйте никаких манипуляций со своими счетами под диктовку неизвестных, кем бы они ни представлялись. Все это может привести к несанкционированному списанию денежных средств с ваших счетов.

2. «Ваш родственник попал в ДТП!»

Злоумышленники звонят под видом родственника – сына, внука, дочери и так далее, либо сотрудника правоохранительных органов, и сообщают, что близкий человек стал виновником ДТП. Незнакомый голос мошенники объясняют плохой связью, полученной травмой, либо, чтобы отвести подозрения, прерывают разговор и передают трубку якобы сотруднику полиции.

Далее они просят передать им деньги якобы для возмещения ущерба потерпевшим либо на лечение пострадавшего родственника. Преступники также могут сообщить, что эта сумма необходима для того, чтобы уголовное дело не возбуждалось. Аферисты убеждают пожилых людей спрятать деньги в пакет и передать их курьеру.

В середине февраля 2024 года поступило сообщение от 88-летней жительницы г. Йошкар-Олы, на стационарный телефон которой позвонил неизвестный и, представившись ее снохой, под предлогом освобождения от уголовной ответственности за совершение ДТП, убедил пенсионерку подготовить свои личные сбережения в сумме 92 тысячи рублей, которые она в дальнейшем передала курьеру – неизвестному мужчине по месту своего жительства.

Меры противодействия: Необходимо провести беседы со своими пожилыми родственниками и рассказать им об этом виде мошенничества. Нужно объяснить, что

прежде всего надо позвонить своим родным и убедиться, что с ними все в порядке, а не отдавать в панике деньги незнакомым людям.

3. Инвестиционное мошенничество

Данный вид мошеннических действий осуществляется под видом привлечения клиентов на инвестиции, в том числе связанные с криптовалютой. Как правило потерпевших уговаривают в ходе телефонных переговоров вложить денежные средства с целью получения прибыли.

Так, в феврале 2024 года в полицию с заявлением обратился 37-летний местный житель. Заявитель пояснил, что нашел в сети Интернет платформу, предлагающую дополнительный заработок на купле-продаже акций различных предприятий. Заявитель установил приложение «Wallet», зарегистрировался на платформе и открыл личный счет, на который под руководством консультанта переводил денежные средства. Аферист посредством мессенджера «Скайп» диктовал инструкцию.

В течение 14 дней местный житель вложил в «инвестиции» собственные сбережения, находившиеся на нескольких картах. Общая сумма переводов достигла порядка 1 млн 858 тысяч рублей. Однако, когда йошкарорец решил вывести свои накопления, ему сообщили, что требуется оплатить страховку. Осознав, что стал жертвой мошенников, потерпевший обратился в полицию.

Меры противодействия: Чтобы обезопасить свои деньги, важно критически относиться к любой поступающей информации. Инвестировать денежные средства можно только на заслуживающей доверия платформе и обладая хотя бы минимальными знаниями по этой теме.

Брокеры, для того, чтобы осуществлять свою деятельность на территории Российской Федерации, должны иметь лицензию на осуществление брокерской деятельности. Такие лицензии организациям выдает Центральный банк РФ. Поэтому первое, что вы должны сделать при выборе брокера, - проверить наличие у него лицензии. Сделать это можно на сайте Банка России. Если у компании, которая обещает вам огромную прибыль, нет лицензии Банка России – осторожно, это мошенники.

На что еще следует обратить внимание:

1. Навязчивые звонки в любое время суток. Помните: профессиональный и честный брокер никогда не станет навязывать свои услуги по телефону. Хорошего специалиста клиенты ищут сами.

2. Обещание брокером баснословной прибыли от вложенных денежных средств. Важно помнить, что ни один брокер не может гарантировать 100-процентное получение прибыли.

3. Отказ назвать адрес сайта брокерской компании. Отсутствие информации о ней в Интернете. Или на сайте компании нет сведений о собственнике компании, юридического адреса и контактных данных.

4. Брокер предлагает быстро открыть счет без проверки ваших документов и заверяет, что достаточно оформить личный кабинет на сайте.

Если вам поступил звонок с предложением об инвестировании, не пожалейте своего времени. Проверьте лицензию, обратите внимание на другие детали, указанные выше. Будьте бдительны, не дайте себя обмануть!

4. Неправомерный доступ к portalу государственных услуг.

В 2023 году стала распространена новая схема, которая заключается в том, что потенциальному потерпевшему от лица сотрудника оператора сотовой связи поступает входящий звонок, в ходе разговора гражданин информируется о том, что срок действия его сим-карты заканчивается и для продления договора необходимо сообщить код из поступившего смс-сообщения. После этого, злоумышленники получают доступ к portalу «Госуслуги», что дает возможность оформления займов на гражданина в различных микрофинансовых организациях.

Так, в феврале 2024 года в дежурную часть МО МВД России «Медведевский» поступило заявление 45-летней жительницы Республики Марий Эл о том, что неустановленное лицо, позвонив на ее абонентский номер, представившись сотрудником компании «МТС», под предлогом продления договора оказания услуг связи, получили коды доступа на портале «Госуслуги». В результате был получен доступ к личному кабинету заявительницы и совершена попытка оформления кредита на сумму 1 млн 234 тысячи рублей.

Меры противодействия:

МВД по Республике Марий Эл призывает жителей региона не выполнять никаких рекомендаций телефонных собеседников!

Важно помнить, что мошенники маскируют номера телефонов, используя SIP-телефонию, подменяя номер на абсолютно любой (на телефоне могут отображаться, в том числе номера банков, различных ведомств, в том числе правоохранительных органов).

5. На популярном интернет-сервисе поиска попутчиков водитель предлагает внести предоплату за поездку по ссылке.

Мошенничество осуществляется с использованием Интернет-ресурса по подбору попутчиков и доставке грузов «BlaBlaCar». Суть преступлений связана с переводом общения в мессенджер «WhatsApp», через который злоумышленник отправляет клиенту подложную ссылку, по которой клиент оплачивает поездку или доставку груза. При этом списание может в значительной мере превосходить договоренную сумму, так как указанные персональные банковские данные на фишинговом ресурсе попадают к злоумышленникам, которые указывают данные на настоящих площадках перевода с карты на карту, подставляя любую сумму для перевода.

Так, в феврале 2024 года в дежурную часть отдела полиции № 3 УМВД России по г. Йошкар-Оле обратилась 38-летняя местная жительница, которая сообщила о том, что неизвестный с помощью популярного интернет-сервиса поиска попутчиков похитил у неё денежные средства.

Полицейские выяснили, что заявительница на Интернет-ресурсе «BlaBlaCar» нашла поездку до г. Чебоксары. Псевдо-водитель предложил ей перевести предоплату и сбросил потерпевшей ссылку. Девушка, перейдя по ней, в платежной форме ввела реквизиты своей банковской карты и код из СМС-сообщения. После чего с её карты списалось более 42 тысячи рублей. Тогда она поняла, что стала жертвой афериста, и обратилась в полицию.

Меры противодействия: Необходимо оплачивать товары и услуги онлайн только на ресурсах, которым вы доверяете. Если от вас хотят оплаты через

конкретный сервис, не переходите по ссылкам в сообщениях. Обращайте внимание на URL-адрес страницы: если он содержит ошибки и неуместные слова или расположен в странной доменной зоне – велика вероятность, что это мошеннический сайт.

Признаки мошенников на «BlaBlaCar»:

- Профиль зарегистрирован недавно;
- У водителя нет фотографии или вместо фото какая-то картинка;
- Низкая цена поездки, чтобы объявления показывались первыми;
- Водитель просит перенести обсуждение из чата в мессенджер;
- С пассажиров требуют предоплату.

6. Мошенничества на сайтах бесплатных объявлений.

Полиция призывает граждан к бдительности при общении через Интернет с незнакомыми людьми. Невнимательность и полное доверие к чужим людям позволяют аферистам обманывать граждан, принуждая их к передаче денежных средств либо сведений, позволяющих похитить сбережения с электронного счета.

В январе 2024 года в дежурную часть УМВД России по г. Йошкар-Оле с заявлением обратился 46-летний местный житель. Он пояснил, что на сайте бесплатных объявлений нашел предложение о продаже автомобильного двигателя и откликнулся. Псевдо-продавец предложил обсудить условия сделки в мессенджере. Заявитель согласился, перевел предоплату и стал ожидать доставку. Мошенник перестал выходить на связь, как только получил денежные средства. Тогда гражданин понял, что стал жертвой злоумышленников. Причиненный ущерб составил 226 000 рублей.

Признаки мошенничества со стороны продавца при покупках в Интернете:

1. Отсутствует адрес и телефон, все общение предлагается вести через электронную почту или программы обмена мгновенными сообщениями.
2. Отсутствует реальное имя продавца, человек прячется за «ником».
3. Продавец зарегистрирован на сервисе недавно, объявление о продаже - единственное его сообщение.
4. Объявление опубликовано с ошибками, составлено небрежно, с использованием транслитерации, без знаков препинания, заглавными буквами и т.д.
5. Отсутствует фото товара либо приложен снимок из Интернета (это можно определить, используя сервисы поиска дубликатов картинок).
6. Слишком низкая цена товара в сравнении с аналогами у других продавцов.
7. Продавец требует полную или частичную предоплату (например, в качестве гарантии, что вы пойдете получать товар на почте с оплатой наложенным платежом).
8. Продавец принимает оплату только на анонимные реквизиты: электронные кошельки, пополнение мобильного телефона или на имя другого человека (родственника, друга и т.д.).

Признаки мошенничества со стороны покупателя при продажах в Интернете:

1. Покупатель не особо интересуется товаром, быстро демонстрирует свое желание сделать покупку и переходит к разговору о способе оплаты.
2. Покупатель просит вас назвать полные реквизиты карты, включая фамилию-имя латиницей, срок действия и CVC-код. При помощи этих данных он сам легко сможет расплатиться вашей картой в Интернете.

3. Покупатель просит вас сообщить ему различные коды, которые придут к вам на мобильный телефон, якобы необходимые ему для совершения платежа.

Как не стать жертвой Интернет-мошенничества:

- следует внимательно изучить информацию Интернет-сайта, отзывы, сравнить цены за интересующий товар. Отсутствие информации, запутанная система получения товара зачастую является признаками мошенничества.

- получить максимум сведений о продавце или магазине, адреса, телефоны, историю в социальных сетях, наличие службы доставки и т.п. Действующие легально Интернет-магазины или розничные продавцы размещают полную информацию и работают по принципу «оплата товара после доставки».

- пользуйтесь проверенными интернет-магазинами, заранее изучайте отзывы других покупателей. Если у вас закрались сомнения по поводу благонадежности продавца, откажитесь от покупки. Если же решили заказать товар, то требуйте от продавца, чтобы посылка оформлялась с описью вложения. Если посылка имеет опись вложения, то она вскрывается до оплаты, содержимое проверяется согласно перечню, подписывается акт, посылка оплачивается, и адресат ее забирает.

- нельзя сообщать (а уж тем более посылать по электронной почте) информацию о своих пластиковых картах. Преступники могут воспользоваться их реквизитами и произвести, например, различные покупки.

Помните, что предоплату за товар вы вносите на свой страх и риск, 100%-ой гарантии получения товара не существует. При заказе товаров внимательно проверяете название сайта в адресной строке браузера, чтобы не попасть на сайт-двойник. Пользуйтесь услугами интернет-магазинов, работающих длительное время и заслуживших положительную репутацию покупателей, читайте отзывы покупателей о работе данных интернет-магазинов.

7. Мошенничества под предлогом получения компенсации за некачественные товары, лекарства или оказанные услуги.

В августе 2023 года в полицию с заявлением обратилась 62-летняя жительница марийской столицы. Она рассказала, как две недели общалась по телефону с людьми, представившими банковскими сотрудниками, которые убедили женщину, что она может получить компенсацию в размере 903 тысячи рублей за ранее приобретенные некачественные биологически активные добавки. Мошенники объяснили, что перед этим нужно оплатить комиссию за перевод денег из-за границы, оформление документов и так далее. Женщина взяла кредиты и перевела 551 000 рублей. Мошенники не остановились и попросили еще 80 000 рублей для присвоения номера поручения на перевод компенсации. Тут уже пенсионерка призадумалась и позвонила в банк, где ей сообщили, что таких поручений не делают. После этого она и обратилась в полицию.

8. Займ денежных средств в социальных сетях.

Злоумышленники взламывают аккаунты знакомых и родственников потерпевших в социальных сетях, после чего от их имени просят одолжить денежные средства на разные цели.

В апреле 2023 года дежурную часть ОП № 2 УМВД России по г.Йошкар-Оле с заявлением обратилась 53-летняя местная жительница. Она рассказала, что в

мессенджере «Телеграмм» от имени приятельницы ей пришло сообщение с просьбой одолжить денежные средства. Введенная в заблуждение потерпевшая, будучи уверенной, что общается со своей знакомой, посредством мобильного приложения перевела почти 21 тысячу рублей. Только спустя некоторое время она узнала, что общалась с мошенниками, которые писали от имени приятельницы.

Меры противодействия: запомните главное правило – в первую очередь необходимо по телефону связаться с родственниками, знакомыми, от чьего имени у Вас просят денежные средства, и убедиться в том, что они действительно нуждаются в помощи!

9. Мошенничество под предлогом возврата найденной вещи

В апреле 2023 года житель Вологды предстал перед судом в г. Йошкар-Оле за то, что брал деньги с людей, потерявших документы или ценные вещи.

Мужчина подыскивал в Интернете объявления о потерянных вещах, связывался с хозяевами и врал, что нашел их. Получив требуемое вознаграждение путем перевода денег, переставал отвечать на звонки. В итоге его жертвами стали 6 человек, в том числе из г. Йошкар-Олы. Всего он взял с граждан 14 тысяч рублей.

Меры противодействия:

- передавайте деньги лично при получении имущества;
- не верьте незнакомцам;
- ни в коем случае не разглашайте конфиденциальную информацию о картах и счетах.

Помните, что ваша безопасность зависит только от Вас!