



МВД России  
Министерство внутренних дел по Республике Марий Эл  
(МВД по Республике Марий Эл) ул. Комсомольская 139, Йошкар-Ола, 424000

«вноября 2022 года № 5/3- \_\_\_\_\_ /3% на №от

Министру образования и науки  
Республики Марий Эл

Л.А. Ревуцкой

424001, Республика Марий Эл, г.ЙошкарОла, ул. Успенская,  
д. 36-а e-mail: minobr@mari-el.m  
О направлении информации

Уважаемая Лариса Анатольевна!

В течение последних лет в связи с развитием телекоммуникационных сетей и информационных технологий широкое распространение приобретают преступления, связанные с хищениями денежных средств граждан, совершаемые с использованием социальной инженерии, Интернет — ресурсов, терминалов оплаты и средств сотовой связи.

Значимым обстоятельством, способствующим росту преступлений данного вида, является виктимность поведения населения — доверчивость либо самоуверенность граждан. Как показывает практика, жертвами преступников становятся люди различных социальных групп, профессий и возрастов. Большинство потерпевших были наслышаны о способах совершения дистанционных хищений, однако сами сообщали всю необходимую информацию преступникам, либо самостоятельно осуществляли операции по переводу денежных средств.

Проблемы противодействия преступлениям, совершаемым с использованием ИТТ, выходят на первый план по актуальности и значимости для обеспечения безопасности всех сфер жизнедеятельности общества.

На территории Республики Марий Эл совершается серия мошенничеств в отношении граждан пожилого возраста по следующей схеме: мошенники совершают телефонные звонки пожилым гражданам на стационарные либо

мобильные телефоны, обращаются к ним от имени либо родственников, либо представителя власти и сообщают о ДТП, виновником или потерпевшим которого стал их родной человек. Для решения проблемы без привлечения виновного к уголовной ответственности или лечения пострадавшего мошенники требуют заплатить денежные средства, за которыми в последующем приезжают водители такси или курьеры.

Так, 21.11.2022 пенсионерка, проживающая в г. Йошкар-Ола передала незнакомому Денежные средства в размере 400 000 рублей ранее незнакомому ей лицу якобы для избежания уголовной ответственности за совершенное ДТП ее внучкой. Перед передачей Денежных средств на стационарный телефон потерпевшей звонила неизвестная Девушка, которая вела эмоциональный разговор и просила передать Денежные средства лицу, который придет к месту ее проживания. При этом, разговаривая с потерпевшей, Девушка не давала отвлечься от разговора и постоянно вела беседу. Таким образом, у потерпевшей не было времени отвлечься и осуществить звонок близким для проверки Действительности событий.

22.11.2022 еще одной пенсионерке позвонила неизвестная Девушка и так же представилась внучкой, которая совершила ДТП и просила передать Денежные средства в размере 800 000 рублей. Однако, потерпевшая, будучи осведомленной о подобных фактах совершения преступления, никаких Действий не предпринимала и сохранила свои сбережения.

Сотрудники уголовного розыска проводят оперативно розыскные мероприятия, направленные на установление подозреваемых в совершении преступлений.

Министерство внутренних дел по Республике Марий Эл напоминает о том, что при поступлении звонка от неизвестного лица на мобильный или стационарный телефон о проблемах близких людей, в том числе при получении смс-сообщений с просьбой о передаче денежных средств, будь то совершение преступления или ДТП, необходимо не впадать в панику и сразу же прервать разговор, после чего лично связаться с родственником по известным номерам телефонов и уточнить информацию. Если с незнакомомго номера неустановленное лицо обращается от имени родственника, необходимо перезвонить на его настоящий действующий номер. В случае, если телефон отключен, принять меры и связаться с коллегами, друзьями или близкими для уточнения информации. Следует помнить о том, что материальный ущерб возмещается в судебном порядке, а не в качестве денежной компенсации незнакомцам.

Популяризация отказа от наличных денег и переход на электронные способы расчетов влечет за собой внедрение

инновационных технологий оплаты. Вместе с тем, растет количество преступлений, совершаемых с использованием конфиденциальных сведений о банковских картах. Из актуальных способов мошенничеств на данный момент можно отметить мошенничество при покупке товаров на сайте частных объявлений «Авито», «Юла» или через социальные сети с использованием сервисов «Безопасная сделка», «Защищенная сделка», а также иных сервисов доставки заказа. Крупные российские сайты имеют удобные для покупателя сервисы, позволяющие доставить товар и обеспечить исполнение двусторонних обязательств. При этом, сайт частных объявлений берет на себя гарантию по обороту денежных средств — продавец не получит деньги до тех пор, пока заказчик не получит посылку в офисе доставки, ровно, как и покупатель не сможет заказать товар, пока не оплатит его стоимость с доставкой. На почве популярности данных сервисов активизировались и мошенники. При ведении переписки с неустановленным лицом на сайте частных объявлений следует не переходить на сайт службы доставки или иные ссылки, которые присылает вторая сторона сделки по причине того, что зачастую мошенниками используются дубликаты форм заказа официальных сервисов доставки, зрительно неотличимых от оригинального сайта. Невнимательный покупатель (продавец) указывает данные своей карты и вводит код подтверждения из смссообщения под предлогом оплаты товара или получения денежных средств за него, после чего мошенники получают платежные реквизиты банковской карты или деньги за несуществующий заказ. Помните о том, что оформление «Безопасной (защищенной) сделки» осуществляется только на сайте площадки объявлений и сервисы доставки не принимают на своих сайтах оплату за товар, если сделка оформлена на площадках частных объявлений, а также не требуют ввода реквизитов банковских карт.

20.11.2022 в УМВД России по г. Йошкар-Оле обратился гр. М., пожелавший приобрести видеокарту для персонального компьютера на сайте «Юла» и вел переписку в мессенджере «WHATSAPP» с неизвестным, который под видом безопасной сделки направил сообщение с генерированной ССЫЛКШ в которой потерпевший ввел реквизиты своей банковской карты и в итоге лишился свыше 10 000 рублей.

Остается распространенной мошенническая схема под предлогом предотвращения несанкционированного списания денежных средств или оформления кредита, Используя добытые различными способами данные физических и юридических лиц, злоумышленники с помощью социальной инженерии осуществляют телефонные звонки с номеров, начинающихся с цифр: 8800, 495, 499, 812, 383 или проводят подмену номеров на официальные

номера банков, правоохранительных органов и иных организаций, информация о которых публично размещена на официальных сайтах. В ходе звонка неустановленные лица представляются должностными лицами банка либо сотрудниками правоохранительных органов, которые якобы желают помочь провести операции по отмене несанкционированного оформления кредита, установить мошенников среди сотрудников банка или предупредить о сбое в системе, блокировке банковской карты, об оплате дорогостоящих товаров, а также осуществлении привязки дополнительного номера телефона и т.п., после чего запрашивается подтверждение на совершение операции, посредством которой граждане сообщают код из смс-сообщения или иные сведения о банковской карте, достаточные для проведения списания денежных средств. Разумнее всего в данной ситуации прекратить разговор и перезвонить в банк по официальному номеру контактного центра банка (номер телефона службы поддержки клиента указывается на оборотной стороне карты). Также можно обратиться в отделение банка лично, где выяснить всю информацию непосредственно у сотрудников банка. Если Вам гарантируют полное погашение задолженности перед кредитно-финансовой организацией, при этом необходимо сразу оформить на себя кредит и оплатить эту услугу, отнеситесь к этому с осторожностью и предусмотрите все риски такого сомнительного предложения. Помните о том, что самый распространенный способ совершения хищений денежных средств с карт граждан — побуждение владельца карты к переводу денег, сообщения данных и иной конфиденциальной информации путем обмана и злоупотреблением доверия.

22.11.2022 пенсионерка, проживающая в п. Медведево лишилась своих сбережений, перечислив 90 000 рублей неизвестным, представившимся лжесотрудниками следственных органов и лжеработников банка, которые осуществили более 10 телефонных звонков потерпевшей и используя методы социальной инженерии (психологические приемы воздействия) убедили совершить операции по переводу Денежных средств.

Министерство внутренних дел по Республике Марий Эл также обращает внимание на участвовавшие случаи мошенничеств под предлогом заработка на инвестиционной платформе. В последнее время отмечается рост сообщений о хищении денежных средств, связанных с попытками граждан заработать путем осуществления торгов на фондовых или валютных биржах, вложения в криптовалюту, а также оформления услуг финансовых агентов, действующих от лица инвестиционных компаний или брокерских фирм. Данные преступления являются наиболее распространенными способами мошенничества в социальном сегменте сети Интернет. В ходе общения неустановленные лица, представляя не существующие организации, предлагают услуги по

управлению инвестициями и брокерскими онлайн-услугами, после чего, используя заманчивые предложения и низкий уровень финансовой грамотности населения, всеми силами стремятся убедить граждан в пополнении счета для начала проведения торговых АКЦИЯМИ, однако вскоре теряют все свои вложения. Мнимый выход на финансовый фондовый рынок, а также подрисовка графиков на сайте компании позволяют гражданам поверить в возможность быстрого обогащения. После внесения минимального депозита на подконтрольный мошенникам счет и регистрации в личном кабинете инвестиционной платформы, лже-брокеры предоставляют клиентам информацию о том, что вклад якобы начал расти. Таким образом злоумышленники побуждают граждан продолжать инвестирование, в редких случаях предоставляя возможность вывести небольшую сумму денежных средств. О том, что инвестиционная платформа является мошеннической, граждане узнают только после неудачных попыток вывести деньги со счета. При столкновении с подобной ситуации надлежит обратить внимание на то, что мошенники, использующие такую схему, предлагают получить высокий доход и умалчивают о возможных рисках, а также настаивают на скорейшем переводе денежных средств. Помимо этого, следует помнить о том, что инвестиционная деятельность ведется только на основании лицензии, наличие которой требуется проверить на официальном сайте Центрального банка Российской Федерации, не доверяя словам лиц, представляющихся брокерами или сотрудниками инвестиционной компании.

17.11.2022 в ОП № 3 умвд России по г. Йошкар-Оле обратилась пенсионерка, пожелавшая получить Дополнительный заработок путем вложения Денежных средств в инвестиции несуществующей компании, рекламу которой злоумышленники разместили в Интернете. От преступных Действий мошенников, потерпевшая лишилась свыше 150 000 рублей, которые перечислила на различные банковские счета.

Приложение: профилактические материалы экз. на 3 л. кие материалы в 1 экз. на 3 в 1

*Уб. А. М. М. М. М. М.*  
*[подпись]*

Врио начальника полиции