



МВД России

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по КЕМЕРОВСКОЙ ОБЛАСТИ – КУЗБАССУ
(ГУ МВД России по Кемеровской
области – Кузбассу)

ул. Н. Островского, 17, г. Кемерово, 650099
тел.(3842) 32-77-53, 32-74-71

23 декабря 2025 г. № 7/2/17-10186
на № _____ от _____

О направлении информации

Ректору ФГБОУ ВО «Кузбасский
государственный технический
университет имени Т.Ф. Горбачева»
Яковлеву А.Н.

650000, г. Кемерово,
ул. Весенняя, 28

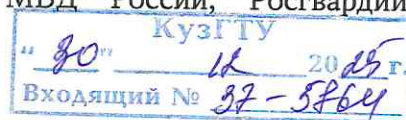
Уважаемый Алексей Николаевич!

Аппаратом Главного следственного управления на постоянной основе проводится анализ обстоятельств, способствовавших совершению отдельных видов преступлений на территории Кемеровской области - Кузбасса, в том числе хищений денежных средств граждан, совершенных с использованием информационно-телекоммуникационных технологий, преступлений, связанных с незаконным оборотом средств платежей и совершение других незаконных финансовых операций, противодействие и предупреждение которых не теряет своей актуальности. Одновременно с развитием телекоммуникационных устройств появляются новые виды «дистанционных» преступлений, позволяющие путем обмана и злоупотребления доверием похитить денежные средства граждан.

Вышеуказанные преступления совершаются путем:

- рассылки сообщений в мессенджерах или размещения рекламы в сети Интернет о легком заработке, с последующим предложением оформить банковскую карту, банковский счет, электронный кошелек на свое имя и передать реквизиты третьим лицам;
- звонка и сообщения о том, что родственники попали в беду с последующим требованием передать денежные средства для оказания им помощи;
- взлома аккаунта в социальных сетях, личного кабинета;
- звонка и сообщения сотрудников ФСБ, Росфинмониторинга, Банка России о том, что установлены подозрительные переводы денежных средств в счет финансирования террористических организаций и вооруженных сил Украины с последующим переводом денежных средств на безопасный счет либо передачи наличных денежных средств курьеру (таксисту) и др.
- предложений инвестирования в различные неблагонадежные высокодоходные проекты;
- размещения объявления о покупке-продаже товаров на различных Интернет-сайтах по заниженной цене;
- рассылки сообщений с текстом «Это ты на фото?» с приложением ссылок для установки на мобильное устройство вредоносных программ;
- размещения рекламы в сети Интернет о легком дополнительном заработке на маркетплейсах, при бронировании отелей, гостиниц;
- взлома мессенджера и рассылки сообщений о просьбе занять в долг.

Помимо этого, с учетом современных реалий, усилена деструктивная идеологическая деятельность иностранных спецслужб, направленная на вовлечение российских граждан, в том числе несовершеннолетних, в противоправную деятельность по подготовке и совершению терактов и диверсий в отношении объектов транспортной и энергетической инфраструктуры, объектов Минобороны России, МВД России, Росгвардии, иных



правоохранительных органов, административных зданий, объектов производства и военно-промышленного комплекса, финансово-кредитной сферы.

В качестве исполнителей преступлений на территории России террористические и экстремистские организации пытаются вербовать, в первую очередь, представителей молодежи из групп риска: оппозиционно настроенных, людей с наркотической зависимостью, детей и подростков, находящихся в сложной жизненной ситуации (например, ставших жертвами мошенничеств, из финансово неблагополучных семей) и др.

Зачастую с целью получения дополнительного дохода граждане находят в мессенджерах объявления, предлагающие заработать на распространении наркотиков, оформлении и передачи за вознаграждение банковских карт третьим лицам (дропперство).

Федеральным законом от 24.06.2025 № 176-ФЗ введена уголовная ответственность за передачу банковских карт иным лицам для осуществления неправомерных операций.

В целях формирования навыков безопасного поведения в информационно-телекоммуникационной сети «Интернет», повышения уровня финансовой грамотности, а также минимизации совершений дистанционных мошенничеств с применением информационно-телекоммуникационных технологий и преступлений в сфере неправомерного оборота средств платежей, предлагаем:

- довести информацию до сотрудников ФГБОУ ВО «Кузбасский государственный технический университет имени Т.Ф. Горбачева» и студентов о недопустимости передачи своих банковских карт, персональных данных своих банковских карт и счетов (CVV-код, ПИН-код, номер карты) третьим лицам; недопустимости обналичивания денежных средств со своих банковских счетов для перечисления или передачи их третьим лицам; недопустимости установки по просьбе третьих лиц на используемые телекоммуникационные устройства различных мобильных приложений и последующего перехода по вредоносным интернет-ссылкам;

- организовать дополнительные профилактические занятия с максимально возможным участием студентов ФГБОУ ВО «Кузбасский государственный технический университет имени Т.Ф. Горбачева», до которых довести информацию о новых способах совершения ИТ-хищений и методике их предупреждения (Приложение №1);

- обеспечить распространение (в помещениях, на информационных стендах, на сайте) ФГБОУ ВО «Кузбасский государственный технический университет имени Т.Ф. Горбачева» информации по предупреждению ИТ-хищений. Профилактические материалы, подготовленные ГУ МВД России по Кемеровской области – Кузбассу, можно скачать по ссылкам: – <https://42.mvd.rf/citizens/профилактика-/profilaktika-distantionnykh-krazh-i-mos>;

- организовать показ профилактического контента, разработанного при участии Следственного департамента МВД России, студентам ФГБОУ ВО «Кузбасский государственный технический университет имени Т.Ф. Горбачева». Подобрать профилактический контент можно перейдя по следующим ссылкам: t.me/internetinsafe (официальный телеграмм канал лиги «Белый Интернет»); <https://vk.com/video/@digitalarmor> (документальный молодежный сериал «Цифровая броня» про мошенничества и кибербуллинг); <https://premier.one/show/vas-bespokoyat-iz-banka?ysclid=mj89jc4q7o551658947> (Документальный сериал «Вас беспокоят из банка» о телефонных мошенниках).

О проведенных мероприятиях и принятых мерах прошу информировать Главное следственное управление ГУ МВД России по Кемеровской области – Кузбассу.

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

С уважением,

Заместитель начальника ГУ –
начальник ГСУ



А.В. Литвинов

исп. А.В. Куценко
(384-2) 32-78-24

**Информация для проведения лекции по теме противодействия
преступлениям, совершаемым с использованием информационно-
телекоммуникационных технологий**

Несмотря на то, что органами внутренних дел Кузбасса на постоянной основе проводится комплексная работа по профилактике различных способов дистанционных преступлений, граждане по-прежнему попадают на уловки злоумышленников.

Продолжают иметь актуальность хищения денежных средств граждан, совершенных с использованием информационно-телекоммуникационных технологий. Одновременно с развитием в данной сфере появляются и новые виды дистанционных преступлений, позволяющие обмануть и присвоить денежные средства граждан.

Дополнительный заработок («дроперство»)

Жертве («дропу») поступает сообщение о легком дополнительном заработке, с предложением оформить на себя банковскую карту, открыть счет или электронный кошелек, но не для личного пользования, а для дальнейшей передачи реквизитов лицам, совершающим преступления (кураторам). Полученные от «дропа» реквизиты банковских карт, счетов, электронных кошельков, мошенники называют потерпевшим, которые самостоятельно, действуя под влиянием обмана, переводят на них свои денежные средства. В дальнейшем «дропы» действуя по указанию мошенников, «обналичивают» денежные средства с использованием различных банкоматов, осуществляют их дальнейший транзит. Использование «дропов» необходимо мошеннику, чтобы самому «не засветиться» в совершении преступления, избежать наказания, скрыть сам факт киберпреступления и легализовать похищенные денежные средства, используя для их вывода цепочку проведенных операций, создавая сложность в установлении лиц, причастных к совершению преступлений.

Мошенники подробно инструктируют своих «подставных лиц», в том числе о том, какие показания должны быть даны в случае задержания сотрудниками полиции в целях избежания уголовной ответственности.

В настоящее время указанные лица («дропы») привлекаются к уголовной ответственности по ст. 187 УК РФ, а также к ним имеется возможность предъявления потерпевшей стороной требования о возврате полученных на их счета денежных средств как неосновательного обогащения, поскольку какие-либо гражданско-правовые отношения между ними отсутствуют. При

получении предложений об оформлении за денежное вознаграждение банковских карт или открытии счетов на свое имя и передаче сведений по управлению счетами или картами другим лицам, необходимо отказаться от таких действий, не становиться соучастником преступления.

Запомните:

1. Отнеситесь внимательно к любым предложениям о трудоустройстве.
2. Если вы ищете работу, лучше обратитесь на официальный сайт компании или специализированные ресурсы.
3. Ни при каких обстоятельствах не передавайте посторонним лицам сведения о своих счетах и банковских картах, а также не совершайте никаких действий со своими картами и вкладами, о которых просят незнакомые лица по телефону.

Родственник попал в беду

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение преступления (совершил ДТП, хранил оружие или наркотики, нанес тяжкие телесные повреждения). Далее в разговор вступает «сотрудник полиции». Он уверенным тоном сообщает, что уже не раз «помогал» людям таким образом и для решения вопроса о не привлечении к ответственности необходимы денежные средства, которые в последствии жертва передает незнакомому человеку или переводит на банковский счет (абонентский номер телефона).

Запомните:

1. Незамедлительно прекратите разговор и свяжитесь со своим родственником и убедитесь в достоверности полученной информации.
2. Не нужно соглашаться на сомнительные сделки по передаче денежных средств.
3. Помните: дача взятки должностному лицу предусматривает уголовную ответственность.

Звонок сотрудника оператора сотовой связи

Мошенники представляются сотрудниками сотовых операторов и предлагают, и даже настаивают на продлении договора обслуживания номера. Для идентификации в системе могут попросить продиктовать паспортные данные и номер СНИЛС. Как только жертва диктует необходимые данные, следом поступает звонок от якобы сотрудника портала «Госуслуги», который сообщает о попытке взлома личного кабинета и для обеспечения защиты просит продиктовать код из СМС-сообщения.

Также, жертве может поступить сообщение в мессенджере или на электронную почту о том, что аккаунт на портале «Госуслуги» взломан и необходимо перезвонить на горячую линию по указанному номеру. Жертва перезванивает на тот номер, который указан в сообщении и диктует код из СМС-сообщения для блокировки аккаунта на портале «Госуслуги».

После передачи кода поступает звонок от якобы сотрудника банка или правоохранительных органов, начиная убеждать, что денежные средства на банковских счетах находятся под угрозой и для этого необходимо снять и перевести их на безопасный счет.

Если сбережений на банковских счетах нет, мошенники сообщают, что от имени жертвы поданы заявки на кредиты, необходимо подтвердить и также перечислить денежные средства на безопасный счет.

Мошенники пропадут, как только поймут, что жертва больше не сможет переводить денежные средства.

Запомните:

1. У SIM-карты нет срока действия. Договор услуги связи является бессрочным.
2. Не доверяйте звонкам, поступившим с неизвестных номеров. Всегда проверяйте информацию по телефону горячих линий, указанных на официальных сайтах организаций.
3. Не выполняйте инструкции незнакомцев, не сообщайте приходящие SMS-коды для подтверждения операций.

Покупка-продажа товаров на различных Интернет-сайтах (Авито, Дром, Юла, социальные сети: Вконтакте, Одноклассники и тд.)

Мошенники размещают объявление о продаже товара по заниженной цене. Когда жертва связывается с продавцом, тот сообщает, что находится в другом городе и предлагает оформить доставку. После чего, мошенник присылает фишинговую ссылку для оформления заказа, которая выглядит точно также, как и легитимный сервис. После ввода данных банковской карты мошенники отправляют ссылку на отслеживание посылки СДЭК по трек-номеру. Однако, трек-номер на официальном сайте СДЭК не отслеживается.

Также, есть ситуации, когда жертва размещает объявление на одном из Интернет-сайтов и на связь выходит мошенник, который изъявляет желание приобрести товар, но так как в данный момент находится не в городе, готов внести предоплату. Мошенник спрашивает номер банковской карты жертвы, чтобы перевести денежные средства, а после просит продиктовать СМС-код из сообщения, которое поступило из банка – якобы это необходимо для банковского перевода. Жертва в спешке называет СМС-код из сообщения, не

успев понять, что это с его банковской карты происходит списание денежных средств.

Запомните:

1. Никогда никому не сообщайте коды из СМС-сообщения или CVV/CVC код карты.
2. Не переходите по ссылкам, не заполняйте ничего на сторонних сайтах.
3. Ориентируйтесь на среднюю для сервиса цену на интересующий вас товар. Мошенники занижают цены, чтобы повысить интерес.
4. Ознакомьтесь с отзывами реальных покупателей, прежде чем оформлять заказ.
5. Проверяйте адрес сайта (ссылку сайта). Обратите внимание на наличие замка в адресном строке браузера, который подтверждает зашифрованное соединение. Если вы видите «http://», а не «https://», это сигнализирует о возможной угрозе.
6. Появились сомнения? Пишите в службу поддержки площадки.

Заработок на инвестициях или игры на бирже

Жертва откликается на рекламное объявление или предложение по телефону. Мошенники могут представляться партнерами инвестиционной программы любого известного банка, пообещать баснословные проценты при минимальных вложениях. Жертву будут уверять, что никаких рисков, прибыль гарантирована, доход можно вывести в любой момент. Все, что потребуется – это заполнить анкету и скачать приложение. Создать личный кабинет поможет персональный менеджер. Далее нужно только внести вложения. Первая же прибыль, которую видит жертва в личном кабинете, снимает остатки сомнений. Мошенники уверяют, что делать нужно крупные ставки, именно тогда доход будет огромным. Потерпевшие безоговорочно верят, берут большие кредиты и совершают переводы. Проблемы возникают, как только жертва пытается вывести прибыль. Тогда оказывается, что нужно пополнить личный счет на такую же сумму. Это ловушка! Мошенники специально создают такие условия, чтобы жертва вкладывала все больше и больше.

Запомните:

1. Прежде всего проявите бдительность и не верьте, что возможно получить большой доход за короткий срок. Ни одна официальная инвестиционная компания таких гарантий не даст.
2. Когда вы пополняете личный счет в банке, то делаете это в приложении банка или в банкомате. Здесь же преступники требуют совершать переводы по разным номерам телефона на имена физических лиц. Так поступают только мошенники.

Рассылка сообщений с текстом «Это ты на фото»?

Пользователям приходит сообщение от знакомых и не знакомых контактов в мессенджере с вопросом: «Это ты на фото»? и к письму прилагается закрытый файл в формате (ФОТО (9).apk).

При переходе по указанной ссылке вместо фотографии автоматически запускается установка вредоносной программы удаленного доступа.

После получения удаленного доступа злоумышленники заходят в банковское приложение и списывают все деньги и оформляют кредиты.

Запомните:

1. Не переходите по подозрительным ссылкам, присланным в том числе от знакомых;
2. В случае если вы уже прошли по ссылке необходимо незамедлительно включить телефон в режим полета, заблокировать банковские карты, отформатировать телефон до заводских настроек для удаления вирусного приложения.

Дополнительный заработок на маркетплейсах (ОЗОН, WB) – лайки, бронирование отелей, гостиниц

Жертве поступает сообщение о легком дополнительном заработке, предлагая забронировать номер в отеле, гостинице, с целью, повышения рейтинга, обещая вернуть стоимость бронирования и оплатить выполненную работу или же продвигать товары на «ОЗОН», «WB» и других маркетплейсах, получая денежные средства за каждый «лайк». Мошенник присылает ссылку, где жертва должна оставить отзыв или «лайк», и просят указать реквизиты банковской карты для перевода оплаты.

Запомните:

1. Отнеситесь внимательно к любым предложениям о трудоустройстве.
2. Не переходите по сомнительным ссылкам и пользуйтесь антивирусными решениями, которые предупреждают о сомнительном характере ресурсов.
3. Если вы ищете работу, лучше обратитесь на официальный сайт компании или специализированные ресурсы.

Взлом мессенджера – занять в долг знакомому

В социальной сети или мессенджере жертве поступает сообщение от знакомого из списка контактов. Он сообщает о том, что у него проблемы и срочно требуются денежные средства, просит выручить небольшой суммой.

При этом, собеседник будет ссылаться на то, что некогда объяснить, для чего потребовались денежные средства, а вместо того, чтобы перевести по мобильному телефону, как правило привязанному к банковской карте, отправит новый номер банковской карты и пояснит, что ту заблокировали.

Запомните:

1. Прежде чем отправлять денежные средства, обязательно перезвоните и уточните просьбу. Убедитесь, что вы общались с реальными владельцами аккаунта.
2. После просьбы о денежном переводе не переходите по ссылкам в сообщениях.
3. Не переводите денежные средства на незнакомые карты, банковские счета, номера виртуальных кошельков, тем более, если они не привязаны к имени просящего.
4. Защитите свой аккаунт: подключите двухфакторную аутентификацию для доступа к нему, не сообщайте никому код авторизации.
5. Используйте уникальный пароль для каждого сервиса.
6. При малейшем подозрении на взлом аккаунта немедленно смените все пароли.

Основные советы, чтобы не стать жертвой мошенников:

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 и т.д.

Не перезванивайте по незнакомым номерам.

Не сообщайте СМС-код из сообщения и номер СНИЛС.

Внимательно проверяйте от кого поступают сообщения.

Возьмите паузу и спросите совета у родных и друзей.

ГСУ ГУ МВД России по Кемеровской области-Кузбассу