МВД России

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по АЛТАЙСКОМУ КРАЮ
(ГУ МВД России по
Алтайскому краю)

пр-т Ленина, д. 74, г. Барнаул, 656015
тел. (385) 239-71-11

10.04.2025 № 4/2848

на № _____ от _____

Ректору ФГБОУ ВО
«Алтайский государственный
педагогический университет»

Лазаренко И.Р.

ул. Молодежная, д. 55,
г. Барнаул, 656031

Вх. отд.
14/04/25

О профилактике преступлений

Уважаемая Ирина Рудольфовна!

В апреле 2025 года в отношении студентки **ФГБОУ ВО «Алтайский государственный педагогический университет»** совершено мошенничество с использованием информационно - телекоммуникационных технологий.

При совершении преступления злоумышленники использовали довольно распространённую схему, состоящую из нескольких этапов:

- на мобильный телефон потерпевшей поступил звонок якобы от сотрудника компании «МТС», который сообщил о необходимости продления срока действия договора на оказание услуг связи и попросил сообщить ему поступивший на мобильный телефон потерпевшей sms-код;

- после того, как потерпевшая выполнила просьбу звонившего, ей стали звонить якобы представители портала «Госуслуги» и ФСБ России, которые убедили потерпевшую в о том, что ее личный кабинет взломан и мошенники пытаются оформить на ее имя кредит, а также в том, что для предотвращения мошеннических действий ей необходимо оформить кредит лично и перечислить полученные в банке кредитные средства на «безопасный» счет;

- находясь под влиянием обмана, потерпевшая поверила мошенникам и выполнила их указания – оформила кредит и перечислила деньги на указанный злоумышленниками банковский счет;

- общая сумма причинённого ущерба составила **185.000 рублей**.

Ранее сотрудниками подразделений ГУ МВД России по Алтайскому краю в Вашей организации неоднократно проводились профилактические мероприятия, направленные на предотвращение таких преступлений в отношении подчиненных Вам сотрудников и студентов, однако, преступления продолжают совершаться.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ» Входящий № 1248/02/01-19 «14» апреля 2025 г.

В целях предотвращения совершения в отношении сотрудников и студентов **ФГБОУ ВО «Алтайский государственный педагогический университет»** мошенничеств и краж, совершаемых дистанционным способом с использованием информационно -телекоммуникационных технологий, направляю Вам рекомендации о правилах поведения граждан, соблюдение которых позволит значительно снизить риск обмана подчиненных Вам сотрудников при контакте с мошенниками.

Такие правила очень просты:

ПЕРВОЕ ПРАВИЛО: не разговаривайте с незнакомыми людьми, кем бы они Вам не представились – родственниками, попавшими в ДТП, сотрудниками компании сотовой связи, банка либо Центрального Банка РФ, ФСБ или полиции, вооруженных сил, социальных служб и т.д.

!!!! Сразу прекратите разговор и при наличии сомнений в достоверности предоставленной информации сами перезвоните Вашему знакомому, в соответствующую организацию либо полицию.

Мошенники в ходе общения с потерпевшими используют средства социальной инженерии, добиваются своего играя на чувствах людей – страхе потерять деньги, переживаниях за близких, желании обогатиться, страхе быть привлеченными к уголовной и иной ответственности за совершение нелегальных финансовых операций (например, перечисление денег гражданам и организациям Украины).

Для того, что противостоять этому влиянию нужно просто ПРЕКРАТИТЬ разговор с мошенником на его начальной стадии. Не нужно проверять на прочность Вашу внушаемость!!! Просто положите трубку!!! А если у Вас возникли сомнения в достоверности предоставленной информации – проверьте ее позвонив родственникам, в банк, оператору связи или в полицию.

ВТОРОЕ ПРАВИЛО: никому, никогда и ни под каким предлогом не отдавайте и не перечисляйте Ваши деньги!!!!

Каждый мошенник, совершающий преступление с использованием абсолютно любого способа преследует цель получить Ваши деньги. Деньги никогда не пропадут с Вашего банковского счета, если Вы сами не отдадите их.

Запомните самое главное – ни один сотрудник банка, полиции, ФСБ и других структур НИКОГДА не попросит вас по телефону перечислить куда бы то ни было Ваши деньги! Запомните это!!!

Запомните главную истину – безопасного счета не существует!

ТРЕТЬЕ ПРАВИЛО: никому и никогда не сообщайте пароли, поступающие на Ваш мобильный телефон.

Под любым предлогом – продлить срок действия сим-карты, сохранить деньги, получить социальное пособие, получить приз – это не имеет значения. **Нужно всегда помнить о том, что такой пароль – это ключ к Вашему банковскому счету**.

ЧЕТВЕРТОЕ ПРАВИЛО: не пытайтесь заработать на инвестициях в сети Интернет и игре на биржах.

Не вкладывайте Ваши деньги в любые инвестиционные проекты, рекламу которых Вы видите в сети Интернет – Вы не получите выгоды, Вас просто обманут, даже в том случае, если от первой якобы сделки Вы получите небольшую прибыль – это обыкновенный крючок.

ПЯТОЕ ПРАВИЛО: если Вы сменили номер телефона – обязательно обратитесь в банк ЛИЧНО и попросите отвязать старый номер от Вашего банковского счета и приложения.

ШЕСТОЕ ПРАВИЛО: не приобретайте товары на непроверенных Интернет-сайтах. !!!! НИКОГДА не приобретайте товары через Интернет с необходимостью внесения предоплаты.

Кроме того, обращаю Ваше внимание, что в настоящее время в крае участились случаи дистанционного мошенничества под предлогом замены счетчиков или установки приложения «ЭНЕРГОСБЫТ». Мошенники убеждают скачать на Ваш телефон вредоносное программное обеспечение, имитирующее официальное приложение «ЭНЕРГОСБЫТ», после чего получают доступа к Вашим персональным данным и похищают денежные средства.

!!!! ПРИЛОЖЕНИЙ С АВТОМАТИЧЕСКИМ ПОСТУПЛЕНИЕМ СВЕДЕНИЙ СО СЧЕТЧИКОВ НЕ СУЩЕСТВУЕТ.

!!! НЕ ПЕРЕХОДИТЕ ПО ПОДОЗРИТЕЛЬНЫМ ССЫЛКАМ И НЕ УСТАНАВЛИВАЙТЕ СТОРОННЕЕ ПРИЛОЖЕНИЕ, ПОРЕКОМЕНДОВАННОЕ НЕЗНАКОМЦЕМ, И НИ ПРИ КАКИХ УСЛОВИЯХ НЕ ПЕРЕДАВАЙТЕ КОДЫ ИЗ SMS-СООБЩЕНИЙ.

!!!!! Если Вам в мессенджере (WhatsApp или Телеграм) поступило сообщение от Вашего руководителя о том, что на Вашем предприятии или в отношении Вас проводятся проверки сотрудниками правоохранительных органов, в связи с использованием Ваших банковских счетов для финансирования террористов и экстремистов -

НЕ РЕАГИРУЙТЕ на поступающие следом за такими сообщения звонки якобы сотрудников полиции и ФСБ – ЭТО МОШЕННИКИ!

СРАЗУ ЖЕ ПРЕКРАТИТЕ РАЗГОВОР И САМИ ПОЗВОНИТЕ ВАШЕМУ РУКОВОДИТЕЛЮ.

И еще ряд более подробных рекомендаций:

- телефонные мошенники рассчитывают на доверчивых и мнительных людей, которые соглашаются с тем, что им говорят и выполняют чужие указания. Если в ходе телефонных переговоров или электронной переписки с неизвестными лицами у Вас возникли сомнения в достоверности

предоставленных Вам сведений – спокойно и уверенно задавайте собеседнику уточняющие вопросы – они отпугнут мошенников и они сами прекратят начатый разговор либо обман станет для Вас очевидным. В период совершения преступлений мошенники всяческими способами пытаются удержать потенциальную жертву в режиме телефонного разговора, не давая возможности прервать разговор, опомнится, в полной мере осознать происходящее и посоветоваться. **Ни при каких обстоятельствах не впадайте в панику!** Прекратите разговор, обратитесь к Вашим родственникам, знакомым либо в полицию и сообщите о происшедшем;

- никогда не сообщайте посторонним свои персональные данные. Помните: сотрудник банка **НИКОГДА** не предложит Вам перевести деньги на какие-либо «безопасные» счета и не попросит предоставить ему информацию, необходимую для доступа к Вашему банковскому счету (номер карты, пин-код, поступившие в sms-сообщениях пароли и т.д.);

- если Вам звонят якобы из банка и просят совершить подобные действия, нужно прекратить диалог. Если у вас возникли вопросы, то можно позвонить в банк по номеру телефона, который указан на оборотной стороне вашей банковской карты, но не перезванивать на тот номер, с которого звонили;

- если Вам звонят и сообщают о том, что мошенники якобы пытаются оформить на Ваше имя кредит либо получить доступ к Вашим банковским счетам – **сразу же прекратите разговор**! Если у Вас остались сомнения – позвоните в банк сами, при наличии поводов беспокоиться – заблокируйте Ваш банковский счет путем личного обращения в банк либо по телефону официальной «горячей» линии;

- если Вам кто-то звонит и просит принять участие в спецоперации, якобы проводимой под контролем сотрудников МВД, ФСБ и других правоохранительных органов – немедленно прекратите разговор (**даже в том случае, если Вам звонят с городских телефонных номеров, официально закрепленных за соответствующими ведомствами**), сообщите о происшедшем в полицию;

- не реагируйте на звонки, поступающие якобы от сотрудников ФСБ, полиции и прокуратуры, которые в ходе телефонных переговоров сообщают Вам об использовании Ваших банковских счетов для финансирования вооруженных сил Украины, а также на другую информацию, касающуюся проведения СВО, угрожая привлечением Вас к уголовной ответственности. **НЕ БОЙТЕСЬ! Не впадайте в панику! Сразу же прекратите разговор и позвоните в полицию**;

- не реагируйте на звонки и сообщения, поступающие якобы от знакомых Ваших родственников, проходящих службу в зоне проведения СВО, с просьбой об оказании материальной помощи. **Дождитесь сеанса связи с родственником, убедитесь в том, что поступившая просьба исходила именно от него;**

- если на Ваш мобильный телефон в социальных сетях (WhatsApp, ВКонтакте, Телеграм и т.д.) поступило сообщение от Ваших знакомых

и родственников с просьбой одолжить деньги и с указанием реквизитов банковской карты для их перечисления - **Прекратите переписку! Деньги не перечисляйте, свяжитесь с Вашими знакомыми по телефону и убедитесь в том, что сообщение поступило именно от них;**

- **НЕ ВКЛАДЫВАЙТЕ** деньги в сомнительные инвестиционное проекты, на Интернет-сайтах которых размещена информация о возможности получения в кратчайшие сроки прибыли, значительно превышающей суммы инвестиций, **даже в том случае, если тот или иной инвестиционный проект Вам порекомендовали Ваши знакомые и родственники** либо его название созвучно или соответствует названию какой-либо крупной и успешной компании;

- если в поисках подработки Вы увидели объявление в сети Интернет либо в социальных сетях с предложением за вознаграждение оценивать товары, реализуемые через известные маркетплейсы – «Wildberries», «ОЗОН» и т.д. – **НЕ РЕАГИРУЙТЕ** на него, в ходе общения мошенники предложат Вам сначала оценивать товары, затем заказывать их с возвращением потраченных средств, а в тот момент, когда Вы начнете доверять им, попросят Вас сделать заказ товара уже на большую сумму, которая Вам **ВОЗВРАЩЕНА НЕ БУДЕТ**!

- осуществляйте поиск работы в сети Интернет только на специализированных сайтах;

- пользуйтесь только проверенными сайтами, порталами и Интернет - магазинами. Простым способом защитить и не потерять свои деньги является оплата товара исключительно после доставки. **Не приобретайте товары, предложения о продаже которых размещаются в группах в социальных сетях и на Интернет-сайтах (например «Одноклассники», «ВКонтакте» и т.д.)**;

- при продаже (покупке) предметов обихода через соответствующие Интернет-сайты не производите по указанию продавцов (покупателей) никаких действий с открытыми на Ваше имя банковскими картами (счетами), в том числе с использованием банкоматов и смартфонов. При необходимости получить оплату просто сообщите покупателю номер открытой на Ваше имя банковской карты либо произведите перечисление денег на указанный последним банковский счет с использованием доступных сервисов. Однако, перед приобретением того или иного товара попросите продавца предоставить Вам подтверждение наличия указанного товара в его распоряжении;

- в случае, если Вам с незнакомого номера позвонил кто-то от имени Вашего родственника (знакомого) и, сообщив о наличии у него каких-либо проблем, попросил прислать на определенный счет либо передать кому-то деньги, **не поддавайтесь панике**, а просто прекратите разговор и перезвоните Вашему родственнику (знакомому) по известному Вам до этого момента номеру телефона, либо позвоните третьим лицам (общим родственникам и знакомым) и проясните ситуацию;

- в случае, если Вам позвонил представитель какой-либо компании (организации) и сообщил о том, что Вам полагаются какие-либо выплаты (за ранее приобретенные медицинские препараты и приборы, в качестве лотерейного выигрыша, возмещение оплаты за ЖКХ и т.д.) – сразу же прекратите разговор и сообщите о происшедшем в полицию;

- в случае, если Вы решили воспользоваться для организации поездки мобильным приложением «BlaBlaCar», предназначенным для онлайн-поиска автомобильных попутчиков, производите оплату за поездку только в приложении, **никогда не переходите по ссылке, предоставленной Вам водителем в целях проведения платежа**. Такие ссылки являются фишинговыми, переход по ним и введение реквизитов Ваших банковских карт в предложенной форме приведет к списанию всех находящихся на Вашем банковском счете денежных средств. Это касается и оплаты товаров на сайтах «Авито» и «Юла» - злоумышленники могут предоставить Вам фишинговую ссылку, якобы для оплаты покупки с использованием сервиса «безопасная сделка», в действительности таким образом мошенники стремятся получить реквизиты Вашей банковской карты для последующего использования их в целях хищения денежных средств с Ваших банковских счетов;

- **не пользуйтесь услугами гадалок**, размещающих информацию о своих экстрасенсорных и сверхъестественных лечебных способностях в сети Интернет. Используемые «гадалками» методы социальной инженерии, основанные, в том числе на устрашении и обещании выполнить невозможное, неизбежно приведут к тому, что Вы, опасаясь мнимых, но кажущихся реальными угроз, передадите злоумышленникам все имеющиеся у Вас сбережения;

- **НЕ ПОЗВОЛЯЙТЕ** Вашим несовершеннолетним детям брать Ваш смартфон с подключенным банковским приложением в Ваше отсутствие, контролируйте действия, которые Ваш ребенок производит с Вашим мобильным телефоном. Мошенники **ИСПОЛЬЗУЮТ ДЕТЕЙ** как инструмент доступа к Вашему банковскому счету, путем обмана убеждая их в ходе телефонных переговоров сообщить номера телефонов родителей, поступившие на абонентские номера последних пароли и коды, в том числе необходимые для получения доступа к их банковским счетам;

- в случае, если Вы решили сменить абонентский номер телефона – **НЕЗАМЕДЛИТЕЛЬНО** после приобретения новой sim-карты обратитесь в банк и отключите прежний номер от банковских счетов либо сделайте это с использованием мобильного приложения банка. В противном случае новый владелец Вашего абонентского номера сможет получить доступ к Вашим банковским счетам и похитить принадлежащие Вам деньги;

- храните открытые на Ваше имя банковские карты, оснащенные функцией бесконтактной оплаты, в надежном и недоступном для третьих лиц месте;

- при совершении покупок в интернет-магазинах уделяйте особое внимание размещенным в сети Интернет отзывам о работе выбранного

магазина; дате создания магазина; проверьте наличие указанного на сайте юридического адреса;

- не стоит доверять сайтам, имеющим в названии знакомые слова, но расположенные в доменных зонах **com.**, **org.**, **biz.**, **net.**, **info.**, **tv.**, **mobi.** и других, не связанных с российским Интернет-пространством;

- если в ходе телефонных переговоров Вы, будучи обманутым, все-таки сообщили мошеннику информацию, достаточную для доступа к вашим банковским счетам, сразу же после окончания разговора позвоните в банк и заблокируйте Ваши банковские карты (счета).

Прошу довести изложенные выше правила поведения до сведения ВСЕХ подчиненных сотрудников и представить в наш адрес информацию о порядке проведенного профилактического мероприятия и числе его участников, а также ведомости об ознакомлении сотрудников с предоставленной профилактической информацией.

С уважением,

Заместитель начальника отдела
главного следственного управления М.В. Дитятева

М.В. Дитятева
(3852) 391-245