ПРАВИТЕЛЬСТВО АРХАНГЕЛЬСКОЙ ОБЛАСТИ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ АРХАНГЕЛЬСКОЙ ОБЛАСТИ

Управление развития системы образования

Троицкий просп., д. 49, корп. 1,
г. Архангельск, 163004
Тел. (8182) 21-52-80, факс (8182) 20-78-17
E-mail: arhobr@dvinaland.ru

09.09.2021 № 209/02-09/8114

На № _____ от _____

Об информировании участников образовательных отношений

Руководителям
муниципальных органов
управления образованием

Руководителям
государственных образовательных
организаций

Руководителям негосударственных
образовательных организаций

Уважаемые коллеги!

В соответствии с письмом УМВД России по Архангельской области от 26 августа 2021 года № 26/821 «О направлении информации» информируем, что с начала 2021 года зарегистрировано более 2000 краж и мошенничеств, совершенных с использованием Интернет-ресурсов и мобильных устройств в отношении студентов и обучающихся.

В настоящее время мошенниками активно используются сайты «двойники», а также обманным путем на мобильные устройства потерпевших устанавливаются вредоносные программы.

Одной из основных мер профилактики подобных преступлений является проведение разъяснительной работы с обучающимися и студентами. Управление МВД России по Архангельской области выражает готовность к сотрудничеству с образовательными организациями по вопросам профилактики киберпреступности.

Просим обеспечить проведение в образовательных организациях профилактических мероприятий по указанной тематике (профилактические листовки, лекционные материалы прилагаются), а также направить контактную информацию представителей УМВД России по Архангельской области по данному вопросу:

заместитель начальника Управления – начальник следственного управления – Зиновьев Александр Владимирович (+7(8182) 217-195);

начальник отдела информации и общественных связей Управления – Распутин Иван Алексеевич (+7(8182) 632-125, 632-124).

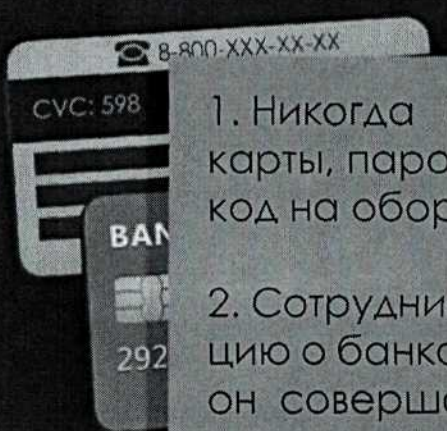
Приложение: в электронном виде.

Заместитель министра –
начальник управления
развития системы образования И.В. Попова

Акишина Евгения Вячеславовна, +7(8182) 201-297

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

УМВД России по Архангельской области предупреждает, в регионе увеличивается количество случаев телефонного и интернет мошенничества.



1. Никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного- и интернет-банка, трехзначный код на обороте карты, коды из СМС.

2. Сотрудники банков никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он совершается якобы с официального номера банка, – дело рук мошенников!

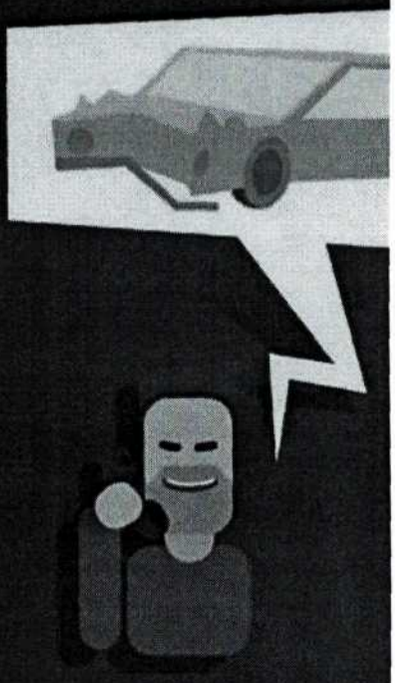
3. Если вам звонят и сообщают о каких-то проблемах с вашим счетом, положите трубку, сами наберите номер телефона банка, который указан на обороте карты, и выясните, все ли в порядке с вашими деньгами.

4. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером!

5. Не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к вам по почте, в соцсетях или в СМС.

6. Знакомый в социальных сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!

7. Поступил звонок, что ваш родственник попал в беду и для решения проблемы срочно требуются деньги? Не паникуйте! Положите трубку и перезвоните родственнику. На самом деле с ним все в порядке. Помните! Попытка дать взятку – преступление!



8. Совершая покупки или продажи в Интернете, на сайтах с бесплатными объявлениями или в интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номера карты.

9. Пользуйтесь только проверенными интернет-магазинами!

10. Используйте лицензионное антивирусное программное обеспечение.

В любой ситуации сохраняйте бдительность и критическое мышление! Не позволяйте мошенникам обманывать Вас!

Если вы стали жертвой мошенников, незамедлительно обращайтесь в полицию по телефону 102 .

Памятка о безопасном использовании банковских карт (счетов)

Распространенный способ совершения хищений денежных средств с карт граждан - побуждение владельца карты к переводу денег путем обмана и злоупотреблением доверия.

Злоумышленники:

-Могут рассылать электронные письма, sms-сообщения или уведомления в мессенджерах от имени кредитно-финансовых учреждений либо платежных систем;

-Осуществляют телефонные звонки (якобы от представителей банка) с просьбой погасить имеющиеся задолженности;

-Под надуманными предлогами просят сообщить PIN- код банковской карты, содержащиеся на ней данные;

-Полученные сведения используют для несанкционированных денежных переводов, обналичивания денег или приобретения товаров способом безналичной оплаты.

Следует помнить!

-Сотрудники учреждений кредитно-финансовой сферы и платежных систем никогда не присылают писем и не звонят гражданам с просьбами предоставить свои данные;

-Сотрудник банка может запросить у клиента только контрольное слово, ФИО;

-При звонке клиенту сотрудник банка никогда не просит сообщить ему реквизиты и совершать какие-либо операции с картой или счетом;

-Никто, в том числе сотрудник банка или представитель государственной власти не вправе требовать от держателя карты сообщить PIN-код или код безопасности;

-При поступлении телефонного звонка из «банка» и попытках получения сведений о реквизитах карты и другой информации, необходимо немедленно прекратить разговор и обратиться в ближайшее отделение банка, либо перезвонить в организацию по официальному номеру контактного центра (номер телефона службы поддержки клиента указан на оборотной стороне банковской карты).

При несанкционированном (незаконном) списании денежных средств рекомендуется:

-Незамедлительно обратиться в кредитно-финансовую организацию с целью блокировки банковской карты или счета для предотвращения последующих незаконных операций с денежными средствами;

-Обратиться в полицию с соответствующим заявлением, в котором необходимо подробно изложить обстоятельства произошедшего с указанием средств, приемов и способов, а также электронных ресурсов и мессенджеров, использованных злоумышленниками;

-Обратиться с заявлением в Роскомнадзор, с изложением обстоятельств произошедшего и указанием интернет-ресурсов, при использовании которых были осуществлены противоправные действия, для рассмотрения вопроса об их блокировке.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

Мошенничество с использованием сайтов-дублеров благотворительных организаций

В сети интернет регулярно размещаются объявления от лица благотворительных организаций, детских домов, хосписов, приютов и др. с просьбой о материальной помощи.

Злоумышленники:

-Создают сайт-дублер, являющийся точной копией оригинального;

-Меняют реквизиты для перечисления денежных средств.

Запомните!
Прежде чем помочь какой-либо организации:

-Позвоните по телефону в указанную организацию;

-Уточните номер расчетного счета, либо посетите ее лично;

-Убедитесь в достоверности размещенной информации.

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

Памятка безопасности при онлайн-покупке товаров и онлайн-оплате услуг

Наиболее часто встречающееся мошенничество при покупке товаров заключается в предложении различных категорий товаров по ценам значительно НИЖЕ, чем среднерыночная цена.

Злоумышленники:

-Создают сайт интернет-магазина и запускают рекламный трафик с целью появления в топе поисковых систем;

-Оплачивают услуги «профессиональных комментаторов», оставляющих положительные отзывы о товарах и работе магазина;

-Требуют полную предоплату за товар, при этом доставка осуществляется исключительно курьерской службой, самовывоз не предусмотрен;

-После перевода денежных средств покупателем перестают выходить на связь, впоследствии могут удалить сайт интернет-магазина.

Характерными чертами интернет-сайтов злоумышленников являются:

-неоправданно низкая цена на товар;

-электронная почта или мессенджеры в качестве способов коммуникации;

-оплата без расчетного банковского счета, отсутствие наименования организации в любой из форм собственности;

-обязательная предоплата, зачастую более половины стоимости товара;

-отсутствие физического адреса расположения магазина или его несоответствие данным интерактивных карт;

-сомнительный интернет-адрес.

Запомните!

-Необходимо выбирать магазин, предлагающий забрать товар самовывозом. При необходимости закажите доставку товара;

-Самый безопасный способ оплаты - после получения заказа;

-Критично относитесь к ситуации, когда менеджер интернет-сайта проявляет излишнюю настойчивость или просит немедленно оплатить заказ под различными предлогами (акционный товар, последний экземпляр, ожидается подорожание продуктовой линейки).

Если Вы стали жертвой мошенников, сообщите об этом в полицию по телефону 02 (со стационарных телефонов) или 102 (с мобильных средств связи) или в дежурную часть территориального органа внутренних дел.

Остерегайтесь мобильных мошенников!

STOP
МОШЕННИК

Прогресс не стоит на месте. Если 15 лет назад общее число абонентов сотовых операторов в России составляло около 300 тысяч, то сейчас, согласно данным статистики, 86% наших соотечественников постоянно используют мобильный телефон.

Не стоят на месте и мошенники. Каждый день они придумывают всё новые схемы, чтобы с помощью мобильного телефона запустить руку в чужой карман. Злоумышленников не интересуют пол, возраст, национальность и социальный статус граждан. Их интересуют только деньги.

В этом буклете вы найдёте информацию о наиболее распространённых способах мобильного мошенничества, а также рекомендации — как не стать жертвой аферистов.

Самые распространенные «уловки» мошенников

Звонки и СМС из банка

Вам звонит сотрудник банка или приходит сообщение о том, что ваша карта заблокирована. Чтобы исправить ситуацию, необходимо позвонить по указанному номеру. Затем под предлогом уточнения информации злоумышленники выясняют данные карты или вынуждают жертву подойти к банкомату, набрать комбинацию клавиш и совершить тем самым операцию по переводу средств.

Взятка

На телефон поступает звонок. Звонивший сообщает, что ваш родственник стал виновником серьёзного ДТП, сейчас находится в отделе полиции, задержан за совершение тяжкого преступления и т.п. Затем мошенник предлагает решить проблему с правоохранительными органами за определённое денежное вознаграждение. Как правило, разговор подкрепляется звуковым сопровождением: вы слышите вой сирены, шум проезжающих машин, голоса. Под разными предлогами поговорить с родственником вам не дают. Вся эта ситуация не более чем хорошо отрепетированный спектакль, цель которого – получить ваши деньги.

Просьба дать позвонить

Всегда с осторожностью относитесь к просьбам «дать позвонить». Мошенник, под предлогом срочного звонка родственникам, может взять ваш телефон, поговорить несколько минут, а затем честно вернуть. За это время с вашего счета исчезает кругленькая сумма, потому что звонок был сделан на платную телефонную линию. Предложите самостоятельно набрать номер телефона и дождитесь соединения с абонентом.

Объявление

Вы подаете объявление об утрате личных вещей или документов с просьбой вернуть их за вознаграждение. На ваш телефон поступает звонок. Собеседник заявляет, что нашел пропавшую вещь и готов её вернуть. В подтверждение вашей заинтересованности просит перевести определенную сумму на электронный кошелек. Это мошенничество! Вы не только не вернете пропажу, но и лишитесь денег.

Выигрыш

Вам приходит СМС или звонят с радио, поздравляют с выигрышем автомобиля или ноутбука и просят отправить подтверждающую СМС, либо внести регистрационный «взнос» через систему электронных платежей, купить карту оплаты и назвать её код. Ни в коем случае не делайте этого.

Просьбы о помощи

Люди поддаются панике, чем и пользуются мошенники. «Мама, положи мне 1000 рублей на этот номер, я потом всё объясню» — распространённое мошенническое сообщение с просьбой о помощи. Злоумышленники надеются на то, что женщина не попытается дозвониться до своего ребенка и, поддавшись панике, положит деньги. Не волнуйтесь. Постарайтесь дозвониться до человека или кого-то из его ближайшего окружения. Лучше чаще звоните близким людям, а не только в день рождения, на Новый год, 8 Марта и 23 Февраля.

Звонок от лица оператора

Вам звонит «техническая служба» оператора связи и предлагает подключить новую услугу, запугивают отключением номера или просят заплатить за услуги роуминга, набрав комбинацию знаков на вашем телефоне.

Поддельный перевод

Абоненту приходит СМС о поступлении на его счет мобильного перевода. Сразу после этого перезванивают жулики, которые излагают легенду, что они по ошибке перевели деньги, и просят их вернуть.

Вредоносные программы

Злоумышленники, маскируя свои программы для смартфонов под полезные, например, счетчики калорий, шагомеры или органайзеры, снабжают их скрытыми вирусами, которые сами отправляют сообщения на платные сервисы. Поэтому не устанавливайте на свой телефон незнакомые программы.

Праздничные открытки

Главным образом в праздники мошенники рассылают сообщения, в которых предлагают перейти по ссылке или отправить СМС с кодом на короткий номер, чтобы получить MMS или праздничную открытку. Просто удалите такое сообщение.

Фальшивый заказ

Мошенники обращаются в службы доставки и делают заказ, как правило, на адрес известной организации. Позже звонят вновь и просят курьера попутно положить деньги на телефон, которые затем собираются вернуть вместе с оплатой заказа. Прибыв на место, доставщик узнаёт, что по указанному адресу никто ничего не заказывал, а положенные на телефон деньги оказались в руках мошенников.

Управление Министерства внутренних дел
Российской Федерации
по Архангельской области

Список мошеннических схем почти безграничен. При этом жулики не стесняются использовать государственную символику и представляться представителями силовых структур, крупных банков и операторов связи для того, чтобы повысить степень доверия потенциальных жертв.

Чтобы противодействовать обману, достаточно знать о существовании мошеннических схем и в каждом случае, когда от вас будут требовать перевести сумму денег, задавать уточняющие вопросы.

Телефонные мошенники рассчитывают на доверчивых, податливых людей, которые соглашаются с тем, что им говорят, и выполняют чужие указания. Спокойные, уверенные вопросы отпугнут злоумышленников. **Чаще звоните родным и близким.**

Листовка, которую вы держите в руках, доступна для скачивания на официальном сайте УМВД России по Архангельской области 29.mvd.ru.

Мы будем благодарны, если вы разместите её на своей странице в социальных сетях, на своём персональном сайте, распечатаете и повесите на информационном стенде в офисе, в подъезде своего дома.

Эта информация поможет другим людям. Помните: предупрежден – значит вооружен.

Если вы стали жертвой мошенников, незамедлительно обращайтесь в полицию по телефону **02**. Кроме того, в УМВД России по Архангельской области работает круглосуточный «телефон доверия» — **216-555**, позвонив по которому граждане могут сообщить имеющуюся у них информацию о готовящихся или совершенных преступлениях.

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ!

УМВД России по Архангельской области предупреждает, в регионе увеличивается количество случаев телефонного и интернет мошенничества.

1. Никогда и никому не сообщайте пин-код банковской карты, пароль от мобильного- и интернет-банка, трехзначный код на обороте карты, коды из СМС.

2. Сотрудники банков никогда не запрашивают информацию о банковской карте. Любой подобный звонок, даже если он совершается якобы с официального номера банка, – дело рук мошенников!

3. Если вам звонят и сообщают о каких-то проблемах с вашим счетом, положите трубку, сами наберите номер телефона банка, который указан на обороте карты, и выясните, все ли в порядке с вашими деньгами.

4. Совершая покупки или продажи в Интернете, на сайтах с бесплатными объявлениями или в интернет-магазинах, будьте осторожны. Не сообщайте лишние данные. Для перевода денег достаточно номера телефона или номера карты.

5. Не переходите по ссылкам в сообщениях от незнакомых людей, которые пришли к вам по почте, в соцсетях или в СМС.

6. Знакомый в социальных сетях просит перевести ему деньги? Обязательно перезвоните человеку, от лица которого поступает просьба. Его аккаунт может быть взломан!

7. Не устанавливайте на мобильные телефоны и компьютеры приложения из непроверенных источников. Есть программы, позволяющие удаленно управлять вашим телефоном или компьютером! Используйте лицензионное антивирусное программное обеспечение.

8. Поступил звонок, что ваш родственник попал в беду и для решения проблемы срочно требуются деньги? Не паникуйте! Положите трубку и перезвоните родственнику. На самом деле с ним все в порядке. Помните! Попытка дать взятку – преступление!

9. В любой ситуации сохраняйте бдительность и критическое мышление! Не позволяйте мошенникам обманывать Вас!

Если вы стали жертвой мошенников, незамедлительно обращайтесь в полицию по телефону 02 или 112. Кроме того, в УМВД России по Архангельской области работает круглосуточный «телефон доверия» - 216-555, позвонив по которому граждане могут сообщить имеющуюся у них информацию о готовящихся или совершенных преступлениях.

Лекционный материал – профилактика мошенничества

Проблема дистанционных преступлений для нашего региона, как и для всей страны в целом, не теряет своей актуальности. Несмотря на постоянную профилактическую работу, с начала 2020 года количество зарегистрированных случаев телефонного и интернет мошенничества и дистанционных краж с банковских счетов граждан в Архангельской области возросла почти на 75%.

1. Наиболее частым способом совершения преступлений является звонок от лица службы безопасности банка. Потерпевшему сообщают, что с его счета совершена попытка несанкционированного списания денежных средств (вариант – на ваше имя пытаются дистанционно оформить кредит). Для предотвращения операции предлагают продиктовать номера банковской карты и коды безопасности, приходящие в СМС-сообщениях. Эти сведения строго конфиденциальны! После их разглашения преступники получают доступ к вашему банковскому счету!

ЗАПОМНИТЕ! Службы безопасности банков никогда не звонят клиентам с сообщениями о проблемах со счетом. Любой подобный звонок – дело рук мошенников. Все вопросы, связанные с обслуживанием вашей банковской карты необходимо решать только по телефону службы технической поддержки, который расположен на оборотной стороне любой банковской карты. Он бесплатный и круглосуточный. Никогда и никому не сообщайте номера и коды безопасности банковских карт!

2. Покупки в сети Интернет. Чаще всего преступления совершаются с использованием сервисов бесплатных объявлений (авито, юла и т.д.) Причем жертвой преступления может стать как покупатель, так и продавец.

- Так при размещении объявления о продаже вещи человеку поступает звонок от потенциального покупателя. Он сообщает, что готов приобрести данную вещь и предлагает внести предоплату. Для перечисления денег просит сообщить данные банковской карты, включая CVV код и коды безопасности из СМС-сообщений. После передачи конфиденциальных сведений со счета потерпевшего происходит списание денежных средств.

- При покупке вещи в сети интернет необходим помнить, что любой дистанционный перевод денежных средств незнакомому человеку потенциально опасен. Вы не можете гарантировать, что он выполнит свою часть сделки. То же касается и не проверенных интернет-магазинов. Вы можете не получить оплаченную вещь, либо получить совсем не то, что заказывали. Пользуйтесь проверенными сервисами и системами безопасного расчета.

3. Большое число преступлений совершается через социальные сети. Чаще всего страницы пользователей взламываются, либо копируются. После чего кругу «друзей» рассылаются сообщения с просьбой дать денег в долг.

Никогда не перечисляйте деньги после просьб в соцсетях. Обязательно созвонитесь с человеком ЛИЧНО.

4. Еще одна преступная схема – предложения от имени известных банков принять участие в розыгрыше и гарантированно получить денежный приз. Для этого необходимо заполнить специальную форму, куда, помимо персональных сведений, необходимо внести конфиденциальную информацию о номерах и кодах безопасности банковской карты. После разглашения данных конфиденциальных сведений со счета потерпевшего списываются денежные средства.

5. Не устанавливайте на телефон неизвестные мобильные приложения. Среди них могут оказаться как вирусные программы, так и сервисы по удаленному управлению телефоном. Если у вас подключены системы дистанционного управления финансами, данные вредоносные программы получат доступ к ним и к вашим сбережениям. Чтобы обезопасить себя, не переходите по сомнительным ссылкам в СМС и ММС сообщениях, не устанавливайте программы, назначение которых вам не понятно, используйте лицензионное антивирусное программное обеспечение!

Будьте бдительны. Не позволяйте мошенникам обманывать вас.