МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«СЕВЕРНЫЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»

Министерства здравоохранения Российской Федерации

ПРИКАЗ

г. Архангельск

«18» 11 2021 г. № 280-ах

О профилактических мерах
по преступлениям, совершенных с использованием
средств мобильной связи и Интернет-ресурсов

На основании письма УМВД России по Архангельской области от 09.11.2021 года № 26/1153, в целях профилактики роста числа преступлений, совершенных с использованием средств мобильной связи и Интернет-ресурсов

ПРИКАЗЫВАЮ:

1. Руководителям всех структурных подразделений университета, заведующим кафедр, деканам факультетов провести разъяснительную беседу с работниками и обучающимися университета с целью недопущения преступлений, совершенных с использованием средств мобильной связи и Интернет-ресурсов, путем доведения, в том числе с применением дистанционных технологий информацию, указанную в Памятках УМВД России по Архангельской области по мошенничеству и кражам (Приложения № 1,2,3,4,5,6,7);

2. Директору ИИЦ Трифонову И.А. разместить на официальном сайте в разделе «Официальные документы» Памятки УМВД России по Архангельской области по мошенничеству и кражам (Приложения № 1,2,3,4,5,6,7) для всеобщего ознакомления в 3-хдневный срок с момента издания настоящего приказа.

3. О принятых мерах по профилактике роста числа преступлений, совершенных с использованием средств мобильной связи и Интернет-ресурсов сообщить в УМВД России по Архангельской области в установленный законном срок, ответственный начальник УПиКО Котлов И.А.

4. Контроль за исполнением данного приказа оставляю за собой.

Ректор Л.Н. Горбатова

Исп.: Верещак Е.В.
Тел.: 28-58-08

Приложение № 1 к приказу
№ 250 ах от 18.11.2021

МВД РОССИИ ПРЕДУПРЕЖДАЕТ

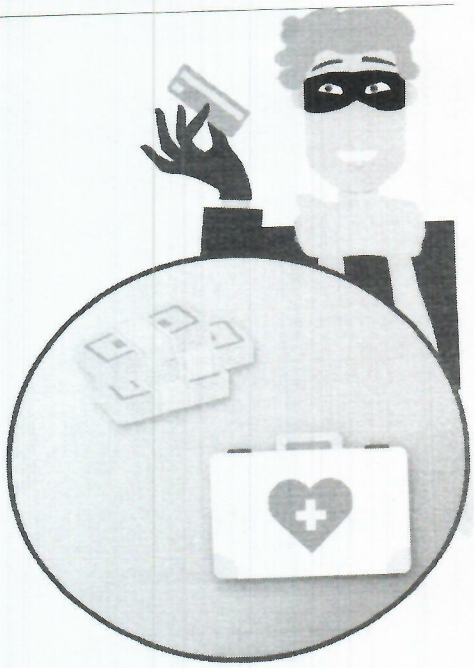
будьте бдительны! звоните 02 или 102

НЕ ОТКРЫВАЙТЕ ДВЕРЬ незнакомым
людям, даже если они представляются работниками социальных, газовых, электроснабжающих служб, полиции, поликлиники, ЖКХ и т.д. Перезвоните и уточните, направляли ли к Вам этого специалиста!

НЕ ДОВЕРЯЙТЕ,
если Вам звонят и сообщают, что Ваш **родственник или знакомый попал в беду** или совершил ДТП, и теперь за него нужно внести залог, штраф, взятку, купить дорогие лекарства - в общем откупиться.
Это ОБМАН!

СЛЕДИТЕ ЗА СОХРАННОСТЬЮ ЛИЧНЫХ ДОКУМЕНТОВ
Аферисты рассказывают, что Вам положены некие выплаты или льготы, а чтобы их получить, надо подписать ряд документов. А вместо этого подсовывают на подпись доверенность или дарственную на Вашу квартиру!

Не подписывайте никакие документы!



Незнакомец сообщает о выигрыше, блокировке банковской карты, о пересчете квартплаты, срочном обмене денег на дому или предлагает приобрести товары и таблетки по низким “льготным” ценам?
НЕ ВЕРЬТЕ - ЭТО МОШЕННИЧЕСТВО!

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ

Вам позвонили/прислали SMS с неизвестного номера с просьбой о помощи близкому человеку

- Не впадайте в панику, не торопитесь предпринимать действия по инструкциям неизвестных людей
- Задайте звонящему вопросы личного характера, помогающие отличить близкого Вам человека от мошенника
- Под любым предлогом постарайтесь прервать контакт с собеседником, перезвоните родным и узнайте, все ли у них в порядке

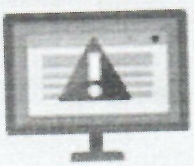
Вам позвонили/прислали SMS «из банка» с неизвестного номера

- Не торопитесь следовать инструкциям и отвечать на запрос
- Не сообщайте персональные данные неизвестным лицам, даже если они представляются сотрудниками банка
- Проверьте информацию, позвонив в контактный центр банка
- Незамедлительно обратитесь в правоохранительные органы

Вам прислали MMS или ссылку с неизвестного номера

- Не открывайте вложенные файлы, не переходите по ссылкам, удалите подозрительное сообщение
- Используйте антивирусное программное обеспечение для телефонов только от официальных поставщиков
- Защитите свой телефон, подключите БЕСПЛАТНУЮ услугу «Стоп-контент»

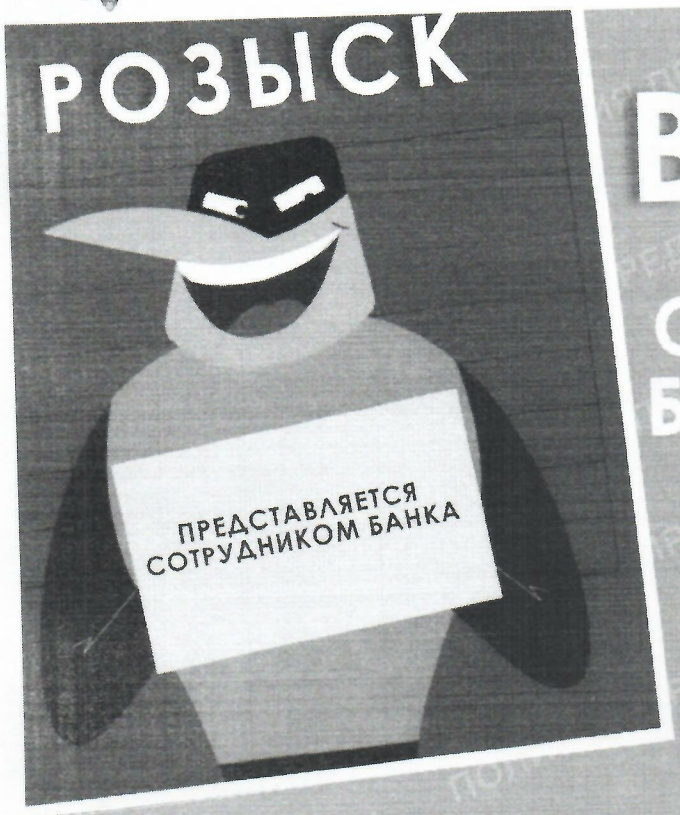
Вы заподозрили интернет-продавца в недобросовестности



- Необходимо оставаться бдительным, не принимать поспешных решений и при первых же подозрениях отказаться от покупки
- Встречаться с продавцом в общественном месте, так как это наиболее безопасный и гарантированный способ покупки. Следует передавать деньги продавцу лично в руки сразу после получения товара
- Никогда не переводить незнакомым лицам деньги в качестве предоплаты

Приложение 1-3
к приказу

УМВД РОССИИ ПО АРХАНГЕЛЬСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ



ВНИМАНИЕ!

СОТРУДНИКИ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА

НИКОГДА

НЕ ЗВОНЯТ

ПО ПОВОДУ ПРОБЛЕМ СО СЧЕТОМ ИЛИ НЕЗАКОННОГО ОФОРМЛЕНИЯ КРЕДИТА

НЕ СОВЕРШАЙТЕ ПОД ДИКТОВКУ ОПЕРАЦИЙ, КОТОРЫХ НЕ ПОНИМАЕТЕ

НЕ ПЕРЕЧИСЛЯЙТЕ ДЕНЬГИ НА ТАК НАЗЫВАЕМЫЕ «БЕЗОПАСНЫЕ» СЧЕТА - ЭТО ОБМАН!

НЕ СООБЩАЙТЕ ПОСТОРОННИМ НОМЕРА И КОДЫ БЕЗОПАСНОСТИ БАНКОВСКИХ КАРТ

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ,
НЕЗАМЕДЛИТЕЛЬНО ОБРАТИТЕСЬ В ПОЛИЦИЮ ПО ТЕЛЕФОНАМ: 02 ИЛИ 112

Приложение № 4
к приказу

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.

Приложение №5
к приказу

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.

Приложение №3
к приказу

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.

Приложение № 2
к Приказу

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 2021 года зарегистрировано почти 2,5 тысячи дистанционных мошенничеств и краж с банковских счетов граждан. Общая сумма ущерба превысила 278 миллионов рублей.

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. 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!

В последнее время вторым по частоте стал звонок от имени службы безопасности банка с сообщением о попытке третьих лиц оформить на Ваше имя кредит. Чтобы это предотвратить, предлагается срочно оформить такой же кредит самому, а денежные средства обналичить и перевести на т.н. «безопасный» счет. Несмотря на очевидную абсурдность ситуации, огромное количество потерпевших идут на поводу у мошенников, оформляют многомиллионные займы и переводят их на номера интернет-кошельков или мобильных телефонов. Печальный рекорд этого года – семейная пара перевела мошенникам почти 8 миллионов рублей.

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.

- При покупке вещи в сети интернет необходимо 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 непроверенных интернет-магазинов. Вы можете не получить оплаченную вещь, либо получить совсем не то, что заказывали. Пользуйтесь проверенными сервисами и системами безопасного расчета.

- 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 код проверки подлинности карты (CVV2,CVC2, CVP2) и коды безопасности из СМС-сообщений. После передачи

конфиденциальных сведений со счета потерпевшего происходит списание денежных средств.

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, кодах безопасности банковской карты, а также ввести код из СМС-сообщений. 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.

Отдел информации и общественных связей
УМВД России по Архангельской области

2021 год