318164 826305

ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПРОКУРАТУРА ЖЕЛЕЗНОДОРОЖНОГО РАЙОНА г. БАРНАУЛА
ул. Крупская, 99а, г. Барнаул, 656049

Ректору ФГБОУ ВО «Алтайский государственный аграрный университет»

Колпакову Н.А.

пр. Красноармейский, 98, г. Барнаул, 656049
agau@asau.ru

Ректору ФГБОУ ВО «Алтайский государственный педагогический университет»

Лазаренко И.Р.

пр. Молодежная, 55, г. Барнаул, 656031
rector@altspu.ru

Ректору ФГБОУ ВО «Алтайский государственный университет»

Бочарову С.Н.

Алтайский край, г. Барнаул, пр-т. Ленина, д. 61

rector@asu.ru

26.12.2022 №Исорг-20010068-1804-22/36-20010068

На № _____ от _____

Руководствуясь ст.ст. 6, 22 Федерального закона «О прокуратуре Российской Федерации» направляю Вам памятки с разъяснениями о способах совершения дистанционных мошеннических действий, а также статью о разъяснении способов мошеннических действий, которые предлагаю разместить на сайтах образовательных организаций.

Приложение: на 3 л.

Прокурор района

старший советник юстиции В.Е. Елизаров

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 00F0021D8FA9C30E5956A9BA37834D2E11
Владелец Елизаров Владимир Евгеньевич
Действителен с 21.11.2022 по 14.02.2024

О.Б. Мухина

ФГБОУ ВО «АлтГУ»
ВХОДЯЩИЙ
№ 10-2-02/5923
28.12.2022

Как уберечь себя от злоумышленников!

Основная масса преступлений — мошенничество.

Рост случаев мошенничества с помощью информационно-телекоммуникационных технологий, а также с использованием мобильного телефона свидетельствует о недостаточной осведомленности граждан в области информационных технологий и пренебрежительное отношение к элементарным правилам безопасности. (Примеры, позвонили из банка, из правоохранительных органов, размещена продажа товара на Авито и др.).

Для предотвращения противоправных действий по снятию денежных средств необходимо исходить из следующего:

Сотрудники банка ни по телефону, ни в электронном письме не запрашивают: персональные данные владельца карты, ее реквизиты и срок действия, пароли и коды из СМС-сообщений, логин, ПИН-код и CVV-код банковских карт. Также не предлагают установить программы удаленного доступа, перейти по ссылке из СМС сообщения, включить переадресацию, под их руководством перевести денежные средства на «защищенный счет».

Необходимо отметить, что при продаже товаров на сайтах Авито, Юла и другие, у продавца / покупателя выбирайте способ оплаты наличными. Если все же придется оплатить по безналичному счету, никогда не следует передать данные банковской карты постороннему лицу.

В случае осуществления заказов на Интернет-ресурсах есть вероятность перехода на поддельный сайт, созданный мошенниками, поэтому обращаю внимание на необходимость использования только проверенных сайтов, внимательного прочтения текстов СМС-сообщений с кодами подтверждений, проверки реквизитов операций и т.д.

Нередко люди попадают впросак, когда мошенники под видом покупателей убеждают жертву сообщить данные банковской карты или подойти к банкомату и подключить доступ их телефона к вашей карте. Но есть и более изощренные способы, например, оформление кредитов на себя, приобретение товаров и т.д.

Нередки случаи совершения мошеннических действий при размещении объявлении о трудоустройстве. Так, сотрудниками полиции за истекший период 2022 года возбуждено 368 уголовных дела по признакам состава преступления, предусмотренного ст. 159 УК РФ.

Установлено, что потерпевшим в поисках работы предлагалось трудоустройство в организации, при этом необходимо приобрести рабочую форму за 4990 руб., якобы в счет заработной платы, указывался адреса потенциального работодателя. После приобретения через курьера рабочей формы, потерпевших отправляли по адресам организации, которым требовались работники, а прибыв по указанным адресам, организации не оказывалось.

Старший помощник прокурора района

младший советник юстиции О.Б.Мухина

Прокуратура Алтайского края информирует!

от действий («телефонных мошенников» пострадало более 8 тысяч жителей края, которым причинен ущерб в размере, превышающем 500 миллионов рублей Будьте бдительны!

Вам звонят сотрудники банка и сообщают о блокировке карты, попытке оформления на Вас кредита, его одобрении, переводе средств на безопасные счета.

Прекратите разговор! Это звонок от мошенников для получения доступа к Вашему счету.

Вы получили СМС-сообщение о неожиданном выигрыше, компенсации, проблемах с банковской картой.

Игнорируйте! По такой схеме работают только мошенники!

Вам звонят из правоохранительных органов или службы безопасности банков с просьбой об участии в выявлении преступника, который похищает средства со счетов граждан.

Вас обманывают! Прервите разговор. Указанные лица не вправе совершать подобные действия. При необходимости с Вами встретятся лично.

Вам звонят и сообщают, что ваш родственник попал в аварию, больницу, совершил преступление. За него нужно внести залог, штраф, дать взятку.

Прекратите разговор. Позвоните родным и знакомым.

На сайте объявлений Вас пытаются убедить, что готовы внести предоплату оплатить покупку, для этого необходимы данные вашей карты.

Будьте внимательны, Вы общаетесь с мошенником!

Вы совершаете покупки в сети Интернет по объявлению или через социальные сети.

До оплаты убедитесь в добросовестности продавца.

Важно знать!

При телефонном разговоре злоумышленники используют различные способы психологического воздействия, чтобы ввести Вас в заблуждение и получить доступ к Вашему счету. Использование современных технологий дает им возможность подмены входящего номера телефона, в том числе на номера органов полиции и иных госучреждений.

Запомните!

Любая просьба о передаче сведений о Вашей банковской карте, сообщений мобильного банка, об оформлении кредита и о перечислении средств — это попытка хищения Ваших денег.

ПАМЯТКА ПО ЗАЩИТЕ ОТ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Способы мошенничества	Чего и зачем добиваются	Способы защиты
Как правило, по телефону от, якобы, сотрудника банка поступает предложение:	1.Напугать возможностью утраты денег.	
- обезопасить деньги на счете, переведя их удаленно на защищенный расчетный счет;	2.Установить доверительный контакт, что позволит получить:	1. Не сообщайте звонящему никаких данных.
- реструктуризировать долг по кредиту;	- номер карты;	2.Прервите разговор.
- установить программу удаленного доступа (или сторонние предложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки;	- срок ее действия;	3.Проверьте информацию, связавшись со своим банком по телефону на оборотной стороне карты или на сайте банка.
- зайти в онлайн-кабинет по ссылке на СМС-сообщения или электронного письма, чтобы узнать о проблеме по счету;	- идентификационный код клиента из 3-х цифр, указанных на обороте банковской карты (CVV или CVC-код);	4.Отслеживайте операции по счету, подключив услугу мобильного банка.
- включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк.	- ПИН-код, дающий возможность совершать операции по счету;	5. При наличии подозрительных операций немедленно звоните в банк.
	-код из СМС-сообщения на мобильный номер, к которому привязана банковская карта, что также обеспечит доступ к деньгам на счете.	6.Помните! Банк может инициировать общение с клиентом только для консультации по предложению собственных услуг.
	3. Похитить деньги.	