ПАМЯТКА

для клиентов БАНКА «МСКБ» (АО) при осуществлении банковских операций (перевод денежных средств, получение кредитных средств, мошеннических действий)

КАК ЗАЩИТИТЬ СЕБЯ ОТ НЕСАНКЦИОНИРОВАННЫХ ПЕРЕВОДОВ

Основные признаки мошенничества:

- **Неизвестные номера.** Звонки с незнакомых номеров, особенно с подменных.
- **Давление и срочность.** Требование немедленных действий, угрозы негативных последствий.
- **Запрос личных данных.** Просьба сообщить пароли, CVV-коды, данные карт.
- **Неожиданные переводы.** Получение денег от неизвестных лиц с просьбой их переслать.
- **Подозрительные ссылки.** Ссылки на поддельные сайты банков или платёжных систем.

Меры предосторожности:

- **Не сообщайте данные.** Никогда не передавайте пароли, CVV-коды и другие конфиденциальные данные.
- **Проверяйте информацию.** Всегда перепроверяйте данные отправителя и получателя.
- **Используйте двухфакторную аутентификацию.** Включите дополнительные уровни защиты.
- **Обновляйте ПО.** Регулярно обновляйте приложения банков и антивирусные программы.
- **Блокируйте карты.** Немедленно блокируйте карту при подозрении на компрометацию.

ЗАЩИТА ОТ МОШЕННИЧЕСКИХ КРЕДИТОВ

Признаки обмана при оформлении кредита:

- **Слишком выгодные условия.** Чрезмерно низкие проценты или отсутствие залога.
- **Давление на подписание.** Уговоры подписать договор без прочтения.
- **Скрытые комиссии.** Неожиданные платежи, не указанные в рекламе.
- **Отсутствие лицензии.** Компания не имеет лицензии ЦБ РФ.
- **Требование предоплаты.** Просьба внести деньги до получения кредита

Действия при подозрении на мошенничество:

- **Прекратите общение.** Немедленно прекратите взаимодействие с подозрительным лицом.
- **Свяжитесь с банком.** Сообщите в банк о подозрительной активности.
- **Проверьте договор.** Внимательно изучите все условия перед подписанием.
- **Обратитесь в полицию.** Сообщите о попытке мошенничества в правоохранительные органы.
- **Информируйте близких.** Предупредите родных о случившемся для их защиты.

ЧТО ДЕЛАТЬ ПОСЛЕ СОВЕРШЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

Экстренные меры:

- **Блокировка карт.** Немедленная блокировка всех банковских карт.
- **Уведомление банка.** Информирование банка о несанкционированных операциях.
- **Заявление в полицию.** Подача заявления о мошенничестве.
- **Обращение в ЦБ РФ.** Подача жалобы через официальный сайт ЦБ РФ.
- **Сохранение доказательств.** Сбор всех доказательств (переписки, записей разговоров).

Профилактика:

- **Регулярный мониторинг.** Отслеживание операций по счетам.
- **Обучение безопасности.** Изучение методов защиты от мошенничества.
- **Информирование окружения.** Распространение информации о новых схемах мошенничества.
- **Обновление контактов.** Регулярная проверка и обновление контактных данных банка.

Помните: ваша бдительность — лучшая защита от мошенников!

МСКБ

МУРМАНСКИЙ СОЦИАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК

ПАМЯТКА

для клиентов БАНКА «МСКБ» (АО) при осуществлении банковских операций (перевод денежных средств, получение кредитных средств, мошеннических действий)

МОБИЛЬНОЕ МОШЕННИЧЕСТВО

Мошенничества с использованием средств сотовой связи совершается, в основном, путем сообщения гражданам заведомо ложной информации.

- Вам сообщают, что кто-то из близких попал в неприятную ситуацию, ему может грозить наказание, и для «решения вопроса» просят передать деньги лично или через терминалы оплаты. **Прекратите общение, свяжитесь со своим и уточните все ли у него в порядке.**
- Приходит СМС о том, что ваша банковская карта заблокирована и, чтобы ее разблокировать, необходимо выполнить ряд действий, не посещая офис банка. **Обратитесь в филиал банка за консультацией.**
- Представившись врачом или сотрудником лечебного учреждения, звонящий сообщает, что у вас или ваших близких серьезное заболевание, для излечения предлагают заплатить деньги или приобрести дорогостоящие препараты и приборы. **Прекратите общение, позвоните в лечебное учреждение и уточните информацию.**
- Вы получаете СМС или звонящий сам сообщает, что вы стали обладателем приза или победителем конкурса. Далее следует просьба перечислить ему деньги под благовидными предлогами, как гарантию того, что награда попадет именно к вам. **Задайте себе вопрос, участвовали ли вы в каком-либо конкурсе, знаете ли вы организацию, которая проводит конкурс, от куда у организации ваши контактные данные. Если вы не смогли ответить хотя бы на один вопрос, проигнорируйте конкурс.**
- Звонящий сообщает лично или присылает смс с просьбой вернуть деньги, которые вам ошибочно перечислены, либо просит срочно пополнить баланс его телефона на небольшую сумму, изображая вашего знакомого. **Прекратите общение и обратитесь в филиал банка за консультацией.**
- Создают фальшивые аккаунты руководителей предприятий в мессенджерах, и отправляют от их имени сообщения, при этом в сообщении может быть, как текст, так и видео с руководителем, изготовленное с помощью искусственного интеллекта. **Прекратите переписку, свяжитесь с руководителем и сообщите ему о том, что мошенники создали поддельный аккаунт с его данными.**
- Представившись представителем оператора сотовой связи, звонящий сообщает, что у вас заканчивается срок договора связи и, чтобы его продлить, необходимо выполнить ряд действий, не посещая офис оператора связи. **Прекратите общение, позвоните оператору сотовой связи по официальному номеру телефона, либо посетите офис продаж.**

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ

Преступники ежедневно придумывают новые схемы и махинации, целью которых является снятие денег со счета владельца карты, чтобы не стать жертвой аферистов, необходимо соблюдать следующие правила.

- Устанавливайте на устройства, к которым привязана карта, только лицензионные программы и обращайте внимание на полномочия, которые вы предоставляете программе при установке, следует исключить доступ к смс и их отправке, доступ к сети интернет и т.д. Мошенники создают программы-вирусы, которые позволяют им получать доступ к данным мобильного банка и похищать деньги с вашего счета.
- Не переходите по ссылкам и не устанавливайте приложения/обновления, поступившие по СМС/ММС/электронной почте/мессенджерам, в том числе от имени банка. Помните, что банк не рассылает своим клиентам ссылки или указания подобным образом.
- В случае потери мобильного телефона с подключенной услугой «мобильный банк», следует срочно обратиться к оператору сотовой связи для блокировки SIM-карты и в отдел банковских технологий по телефону 8-815-223-09-14 для блокировки самой услуги, либо при посещении банка и подачи соответствующего заявления. При смене номера телефона необходимо подать заявление в банк или в электронном виде в услуге «мобильный банк».
- Никогда не передавайте свою карту третьим лицам и не позволяйте им совершать с ней манипуляции, не называйте посторонним, даже если они представились сотрудниками банка, полные данные о своей карте: номер, ФИО владельца, срок действия, код проверки. Сотрудники банка никогда не спрашивают такую информацию. Храните ПИН-код и карту раздельно, а лучше – запомните ПИН-код наизусть.

Напоминаем Вам, что в соответствии с №41-ФЗ от 01.04.2025, сотрудники БАНК «МСКБ» (АО) не используют мессенджеры (WhatsApp, Telegram и т.п.) для общения с клиентами. Остерегайтесь МОШЕННИКОВ!

МСКБ

МУРМАНСКИЙ СОЦИАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК

ПАМЯТКА

для клиентов БАНКА «МСКБ» (АО) при осуществлении банковских операций (перевод денежных средств, получение кредитных средств, мошеннических действий)

ВСЁ О ДРОППЕРСТВЕ И КАК ИЗБЕЖАТЬ ВОВЛЕЧЕНИЯ В ПРЕСТУПНУЮ СХЕМУ

Дроппер (или дроп) — это человек, которого мошенники используют для обналичивания или перевода денег, полученных преступным путём. Дропперы могут участвовать в схеме как осознанно, так и неосознанно, но в любом случае несут ответственность перед законом.

Как работают дропперы

Основные действия дропперов включают:

- Получение денег на свою банковскую карту.
- Обналичивание средств.
- Перевод денег на другие счета.
- Предоставление доступа к банковскому счёту.
- Обмен денег на криптовалюту.

Кто становится дроппером

Группы риска:

- Подростки старше 14 лет.
- Студенты.
- Пожилые люди.
- Люди, нуждающиеся в быстром заработке.
- Те, кто уже пострадал от мошенников.

Основные схемы вовлечения

Популярные методы вербовки дропперов:

- **Объявления о работе** с привлекательными условиями (быстрый заработок, удалённая работа).
- **Ошибочный перевод** — просьба вернуть деньги на другой счёт.
- **Помощь у банкомата** — просьба снять деньги для незнакомца.
- **Предложения от банков** — оформление карт для выполнения плана.
- **Знакомства в интернете** с последующим предложением лёгкого заработка.

Как не стать дроппером

Правила безопасности:

- Не делитесь паролями и данными банковских карт.
- Не переходите по подозрительным ссылкам.
- Не называйте коды из СМС.
- Проверяйте кредитную историю.
- Не соглашайтесь на сомнительные предложения заработка.
- При неожиданных переводах обращайтесь в банк.
- Не помогайте незнакомцам с банковскими операциями.

Ответственность за дропперство

Уголовная ответственность включает:

- Лишение свободы до 7 лет.
- Штраф до 1 миллиона рублей.
- Возмещение ущерба пострадавшим.
- Блокировка банковских счетов.
- Включение в реестр дропперов.

Что делать при подозрении на мошенничество

Действия при опасности:

- Немедленно свяжитесь с банком.
- Сообщите о подозрительных предложениях в полицию.
- Обратитесь на горячую линию Банка России (8-800-300-30-00).
- Предупредите близких о рисках дропперства.

Помните: незнание законов не освобождает от ответственности. Всегда сохраняйте критическое мышление и не доверяйте сомнительным предложениям легкого заработка.

МСКБ

МУРМАНСКИЙ СОЦИАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК