



Минфин
России

мои финансы

Всероссийская просветительская Эстафета
по финансовой грамотности

Этап: «Финансовая безопасность
для всей семьи: защити свои деньги»



ГАЙД

ТОП-5 САМЫХ АКТУАЛЬНЫХ СХЕМ ТЕЛЕФОННЫХ МОШЕННИКОВ

СХЕМА 1. Меняем медицинский полис

Мошенник под видом сотрудника страховой компании сообщает, что у вас истек срок действия медицинского полиса. Документ нужно заменить. Для этого назовите код из смс, который придет на телефон.

Работники страховых компаний не просят устанавливать приложения или называть им коды из смс и данные. А медицинский полис действует бессрочно, и его не нужно менять.

СХЕМА 2. Вам цветы, примите доставку!

Мошенник под видом курьерской службы сообщает, что вам отправили букет, уточняет, куда и когда его привезти. После получения букета курьер просит назвать код из смс, чтобы подтвердить доставку заказа.

Курьерские службы не просят коды из смс для подтверждения доставки. Свяжитесь с отправителем подарка и уточните детали. Если это сделать не удастся — не принимайте презент.

СХЕМА 3. Получите письмо!

Мошенник под видом сотрудника «Почты России» сообщает, что вам пришла посылка/ заказное письмо. Для его получения надо воспользоваться несуществующим чат-ботом и ввести код из смс.

Сотрудники «Почты России» никогда не звонят клиентам и не запрашивают код из смс. Вы можете самостоятельно подключить или отказаться от услуг сервиса на его официальном сайте или в приложении.

Подробнее на портале
моифинансы.рф



СХЕМА 4.

Заканчивается договор сотовой связи

Мошенник под видом оператора сотовой связи сообщает, что у вас заканчивается контракт на мобильную связь. Его нужно продлить, иначе вы не сможете звонить, отправлять смс и пр. Это можно сделать через «Госуслуги»: просто продиктуйте код из смс.

Сотрудники оператора могут отключить связь, если вы не оплачиваете услуги или ваши персональные данные, указанные в договоре, необходимо актуализировать. Но это произойдет не сразу. Вы можете обновить данные не только через «Госуслуги», но в салоне связи.

СХЕМА 5. Зафиксирована подозрительная операция по вашей карте!

Мошенник под видом сотрудника банка сообщает, что по вашей карте зафиксирован подозрительный перевод или кто-то пытается оформить кредит на ваше имя. Для отмены этих финансовых операций вы должны назвать код из смс, который направит специалист.

Сотрудники банков, правоохранительных органов и государственных ведомств не звонят гражданам и не запрашивают у них персональные данные, коды из сообщений. Положите трубку и позвоните в организацию, по номеру с ее официального сайта.

БУДЬТЕ БДИТЕЛЬНЫ! Если вас просят назвать код из СМС, не поддавайтесь на уговоры. Мошенники могут придумывать разные предлоги, чтобы выманить его. Этот код дает доступ к вашим персональным данным и банковским счетам.



Минфин
России

мои финансы

Всероссийская просветительская Эстафета
по финансовой грамотности

Этап: «Финансовая безопасность
для всей семьи: защити свои деньги»

ИНСТРУКЦИЯ. ВЗЛОМАЛИ «ГОСУСЛУГИ»: ЧТО ДЕЛАТЬ



Вы обнаружили, что ваш аккаунт на «Госуслугах» взломан.
Что делать? Следуйте шагам, описанным в нашей инструкции, чтобы защитить свои данные.

ШАГ 1. Восстановите доступ к учетной записи и замените пароль

Злоумышленники рассылают сообщения от имени государственных и финансовых организаций, интернет-магазинов, организаторов лотерей и даже родственников и близких. Их цель — заманить жертву на фишинговый сайт, чтобы украсть ее личные данные, информацию о банковской карте и деньги.

Если мошенники ИЗМЕНИЛИ контактные данные

Лично в центре обслуживания

Предоставьте специалисту МФЦ паспорт, СНИЛС и номер телефона. Он поможет восстановить доступ к «Госуслугам».

Подробнее
на портале
моифинансы.рф



Если мошенники НЕ ИЗМЕНИЛИ контактные данные

Онлайн на «Госуслугах»

На странице входа в аккаунт нажмите **«Восстановить доступ»**. Выберите, куда придет код подтверждения для смены пароля:

- на номер телефона → 4 цифры в смс,
- на электронную почту → ссылка для подтверждения на создание нового пароля.

Сервис может запросить данные для подтверждения личности: паспорт, ИНН или СНИЛС.

Онлайн через банки Сбер, Почта Банк или РНКБ, если вы являетесь их клиентом.

Зайдите на сайт или в приложение банка и пройдите шаги по подтверждению учетной записи на «Госуслугах».

Важно: данные паспорта на «Госуслугах» должны совпадать с данными в банке.

ШАГ 3. Проверьте, где мошенники могли использовать учетную запись

В личном кабинете выберите раздел **«Безопасность»** → вкладка **«Действия в системе»**. Если злоумышленники успели подать заявления в МФО, отзовите их.

ШАГ 4. Убедитесь, что на вас не оформили кредит

Выберите услугу «Получение информации о хранении вашей кредитной истории» и закажите отчет в бюро кредитных историй (БКИ). В присланных документах посмотрите, какие заявки на кредиты подавались от вашего имени.

Важно: Если на вас взяли кредит — срочно обратитесь в банк или МФО и сообщите, что заявку на кредит подали мошенники.

ШАГ 5. Защитите свою учетную запись

Вы можете выбрать один из дополнительных способов или подключить все три:

- Настройте вход с дополнительным способом подтверждения, помимо пароля: добавьте одноразовый код или вход с помощью биометрии.
- Установите контрольный вопрос.
- Подключите уведомление с помощью письма на электронную почту о входе в личный кабинет.

ШАГ 2. Выйдите из учетной записи на «Госуслугах» со всех устройств, кроме текущего

В личном кабинете выберите раздел **«Безопасность»** → вкладка **«Действия в системе»** → **«Выйти»**. Повторите то же самое во вкладке **«Мобильные приложения»**, нажмите **«Выйти»** из тех приложений, в которые вы не входили.

ШАГ 6. Обратитесь в МВД

Сообщите полиции, что вашу учетную запись взломали. Подать заявление можно лично или онлайн на сайте МВД.



ПАМЯТКА

Я ДРОППЕР?

Проверьте, не попали ли вы в ловушку
финансовых мошенников

ДРОППЕР — это человек, которого
мошенники используют для вывода
и обналичивания похищенных денег.



ЧТО ДЕЛАЕТ ДРОППЕР

- Оформляет на себя банковские карты и отдает доступ к ним мошенникам.
- Переводит деньги на разные счета по указанию преступников.
- Снимает и вносит в банкоматы украденные деньги.
- Предлагает работу с «дополнительным» взносом, который нужно перечислить «работодателю».
- Делает «ошибочные» денежные переводы гражданам.
- Рассылает сообщения о выигрыше, который якобы выпал потенциальной жертве мошенников.

ГДЕ ПРЕСТУПНИКИ ВЕРБУЮТ ДРОППЕРОВ

Рассылают предложения
о трудоустройстве:

- В социальных сетях.
- В мессенджерах.
- По электронной почте.
- Расклеивают объявления и раздают листовки в общественных местах.

В зоне риска
подростки
и студенты,
которые хотят
быстро
заработать!

ВНИМАНИЕ!
Дроппером можно
стать случайно!



КАК НЕ СТАТЬ ДРОППЕРОМ

- Будьте осторожны с предложениями о работе, связанными с переводами денег.
- Будьте осторожны с вакансиями, которые предлагают легкую прибыль без усилий, навыков и образования.
- Не открывайте банковские карты по просьбе незнакомых людей.
- Не передавайте никому реквизиты своей карты.
- Не возвращайте деньги, которые пришли на ваш счет или телефон «по ошибке», а отправитель требует вернуть их на другой счет.
- Не верьте звонкам от «сотрудников» правоохранительных органов или Банка России.

Подробнее
о дропперах
читайте на

moifinansy.rf



ВНИМАНИЕ! Участие в дропперской схеме — уголовно наказуемое преступление, ответственность за которое граждане несут с 14 лет. Незнание своей вовлеченности в преступление не освобождает от ответственности за него.



ПАМЯТКА

ЧТО ДЕЛАТЬ, ЕСЛИ СТАЛ ДРОППЕРОМ

Дроппер может не знать, что он стал соучастником преступления. Если вы вдруг поняли, что стали дроппером, сделайте следующие **7 шагов**. Они помогут минимизировать неприятные последствия.

ШАГ 1

Заблокируйте карту или счет,

которые использовались в мошеннических операциях.



ШАГ 2

Не общайтесь с мошенниками

Прекратите любые действия, связанные с мошеннической схемой. Не выполняйте больше никаких поручений и не передавайте деньги или данные.



ШАГ 3

Сообщите в банк

Свяжитесь с вашим банком и объясните ситуацию, расскажите о подозрительных операциях. Сотрудники примут меры, чтобы вернуть деньги пострадавшим.



ШАГ 4

Обратитесь в правоохранительные органы

Напишите заявление в полицию. Предоставьте доказательства: записи разговоров, сообщения, данные о переводах.



ШАГ 5

Проконсультируйтесь с юристом

Он разъяснит, какие правовые последствия могут быть и как действовать.



ШАГ 6

Подготовьтесь к проверке

Будьте готовы предоставить правоохранительным органам всю необходимую информацию и сотрудничать с расследованием.



ШАГ 7

Не повторяйте ошибок

В будущем будьте более осторожны с предложениями о легком заработке, особенно если они связаны с банковскими операциями или передачей денег.



Подробнее
о дропперах
читайте на
moifinansy.rf



ПОМНИТЕ! Своевременные действия помогут избежать серьезных проблем и привлечь мошенников к ответственности.