ваши личные
финансы
семейный журнал
№3 (177)

Личные финансы и цифровая среда

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

СПЕЦВЫПУСК

Как защитить свои персональные данные, деньги и имущество от мошенников

ваши личные финансы

№3 (177)
СПЕЦВЫПУСК

Деловой вестник
«Ваши личные финансы» —
семейный журнал о финансах

сайт: vlfin.ru
e-mail: info@vlfin.ru
Адрес редакции:
634029, г. Томск,
ул. Гоголя, 15, оф. 401
тел.: (3822) 716-797, 716-787
По вопросам размещения рекламы:
тел.: 716-797

Руководитель проекта главный редактор Оксана В. Кудрявцева
Выпускающий редактор
Юлия ФАЛЛЕР
Литературный редактор
Юлия АЛЕЙНИКОВА
Дизайн-макет
Илья МЯСНИКОВ, Анна ЦЫРФА
Верстка Никита БИРЮКОВ

Издается с 2010 года.
Учредитель и издатель
ООО «Р-консалт», 634029, Томск,
ул. Гоголя, 15, оф. 401.
Зарегистрирован Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Томской области.
Свидетельство о регистрации
ПИ № ТУ 70-00344 от 1 сентября 2014 г.

Отпечатано в типографии
АО «Советская Сибирь»,
630048, Новосибирск,
ул. Немировича-Данченко, 104.
Тираж: 4 000 экз.
Дата выхода в свет: 06.08.2026.
Время подписания в печать:
по графику — 20.00, 31.07.2026.
фактически — 20.00, 31.07.2026.

Мнение редакции может
не совпадать с мнением авторов.

Цена свободная.

Спецвыпуск тематического номера семейного журнала «Ваши личные финансы», направленного на формирование у населения устойчивых компетенций в сфере цифровой и финансовой безопасности.

12+

В этом выпуске

СОВРЕМЕННЫЕ СХЕМЫ ФИНАНСОВОГО МОШЕННИЧЕСТВА ОСНОВАНЫ НА ДВУХ ВЗАИМОСВЯЗАННЫХ СОСТАВЛЯЮЩИХ — СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ТЕХНОЛОГИЯХ, КОТОРЫЕ ДЕЛАЮТ ОБМАН НЕОТЛИЧИМЫМ ОТ ПРАВДЫ. НО **КАКИМИ БЫ СОВЕРШЕННЫМИ НИ БЫЛИ БАНКОВСКИЕ СИСТЕМЫ, КАКИЕ БЫ МЕРЫ НИ ПРЕДПРИНИМАЛИСЬ СО СТОРОНЫ ГОСУДАРСТВА, САМЫМ СЛАБЫМ ЗВЕНОМ ВСЕ ЖЕ ЯВЛЯЕТСЯ ЧЕЛОВЕК.** РАЗБИРАЕМСЯ, КАКИЕ ИМЕННО СЛАБОСТИ ИСПОЛЬЗУЮТ МОШЕННИКИ И КАК СЕБЯ ВЕСТИ, ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ.

Как социальная инженерия и технологии крадут у нас деньги

текст:
Оксана КУДРЯВЦЕВА,
Юлия СОЛОВЕЙ

Социальная инженерия: искусство психологического взлома

Злоумышленники прекрасно знают «болевые точки» людей и используют их. В большинстве случаев успех атак напрямую связан с психологическим воздействием на жертву. Это и есть социальная инженерия, а главные человеческие триггеры — это эмоции. Тщеславие, злость, жадность, желание помочь, чувство вины, страх за репутацию, перспектива быстрой финансовой выгоды, ощущение уникальной возможности, которую нельзя упустить, желание получить «секретный доступ» — именно на этом играют мошенники.

Чтобы усыпить бдительность человека, жулики предварительно собирают информацию о нем, используя утечки из баз данных и мессенджеров. Существует целая система анализа персональных данных потенциальных жертв обмана — доксинг: мошенники собирают сведения, которые помогут втереться в доверие, шантажировать, вымогать или выманивать деньги. Поэтому они обращаются к жертве по имени, знают адрес, дату рождения и даже историю последних покупок. Это создает у человека иллюзию, что он разговаривает с настоящим представителем организации, от имени которой позвонили.

Ни статус, ни деньги, ни знания не избавляют от риска оказаться жертвой мошенника.

Защищает только привычка сомневаться, критически оценивать информацию и проверять ее, а также способность вовремя остановиться, не действовать сгоряча.

Преступники постоянно меняют тактику и модифицируют способы обмана. Люди перестали отвечать на звонки с незнакомых номеров — злоумышленники переключились на мессенджеры, электронную почту и соцсети. Через них они рассылают сообщения с какой-то цепляющей информацией — например, о выигрыше денежного приза или о полагающейся социальной выплате, побуждая перейти по ссылке «для получения выигрыша», «оплаты пошлины» и прочее.

Так реализуются схемы фишинга (от англ. fishing — рыбная ловля), нацеленные на выуживание у пользователя конфиденциальной информации: платежных данных банковской карты, логина и пароля от онлайн-банка. За такими ссылками могут скрываться и вредоносные файлы: переход по ссылке загружает на устройство жертвы вирус или программу, которая дает мошенникам доступ к данным на смартфоне, логинам и паролям от банковских приложений или вообще полный контроль над гаджетом. А значит, жулики смогут украсть все деньги или же использовать конфиденциальную информацию для шантажа.

Как показывает практика, никто из нас не застрахован от манипуляций подкованных в психологии мошенников. Ни статус, ни деньги, ни знания не избавляют от риска оказаться их жертвой. Защищает только привычка сомневаться, критически оценивать информацию и проверять ее, а также способность вовремя остановиться, не действовать сгоряча. Потому что именно на это нацелена социальная инженерия — взломать человека психологически, не дать ему включить голову и спокойно подумать.

Спуфинг и дипфейки: от психологии к технологиям

Для усиления эффекта психологических манипуляций мошенники все чаще используют цифровые технологии — программную маскировку и искусственный интеллект. С помощью программы злоумышленник подменяет на экране смартфона жертвы реальный номер звонящего фальшивыми данными. Так он убеждает жертву, что с ней общается представитель банка или правоохранительных органов, а затем в ход идет уже социальная инженерия.

Такой вид кибермошенничества называется спуфингом (от англ. spoof — подделка, обман). Его цель такая же, как и у фишинга, — получить доступ к персональным данным, заразить устройство жертвы вирусом или заставить отдать деньги. Другая схема спуфинга — рассылка текстовых уведомлений от имени известных компаний. Уведомления содержат опасную ссылку, ведущую на поддельный ресурс, где жертву просят ввести учетные данные или платежную информацию.

Правила защиты от спуфинга

- Проверяйте информацию из сообщений, звонков и писем, в которых вас просят совершить финансовые операции.
- Не отвечайте не звонки с незнакомых номеров и запретите прием звонков от неизвестных контактов в мессенджерах.
- Не переходите по ссылкам из СМС, электронных писем и сообщений в мессенджерах, присланных непонятно кем, не скачивайте файлы, которые вам предлагают загрузить в таких сообщениях.
- Не вводите реквизиты карты и учетные данные (логины и пароли) на сомнительных сайтах.
- Используйте антивирусную программу на всех устройствах.
- Регулярно обновляйте свои устройства, чтобы операционная система получала актуальные настройки безопасности от разработчика.

Самый технологичный обман на сегодня — это дипфейки (от англ. deep learning — глубокое обучение и fake — обман, подделка) — реалистично подделанные с помощью нейросетей фото, видео или голосовые записи. Так, для создания голосового дипфейка достаточно короткой записи голоса. Искусственный интеллект «считает» его характеристики, манеру речи человека и скопирует их. После чего мошенник сможет озвучить любой текст этим голосом и от имени его владельца разошлет родственникам и знакомым «скопированного» голосовое сообщение с просьбой перевести деньги или сообщить необходимые данные.

Так как количество дипфейков растет, очень важно следить за тем, что мы выкладываем в интернет. Известен случай, когда человеку позвонили якобы из отеля, который он забронировал на отпуск. Уточнили, когда он летит, вычислили, в какое время будет в самолете, и пока он был вне зоны доступа, рассылали его знакомым через мессенджер «кружочки»: якобы мужчина попал в аварию и ему срочно нужны деньги. Дипфейки сегодня настолько качественные, что распознать обман непросто. Поэтому и здесь важно проверять информацию: связываться по альтернативным каналам с человеком, от имени которого пришла просьба перевести деньги, и спрашивать, действительно ли он просил у вас финансовой помощи.

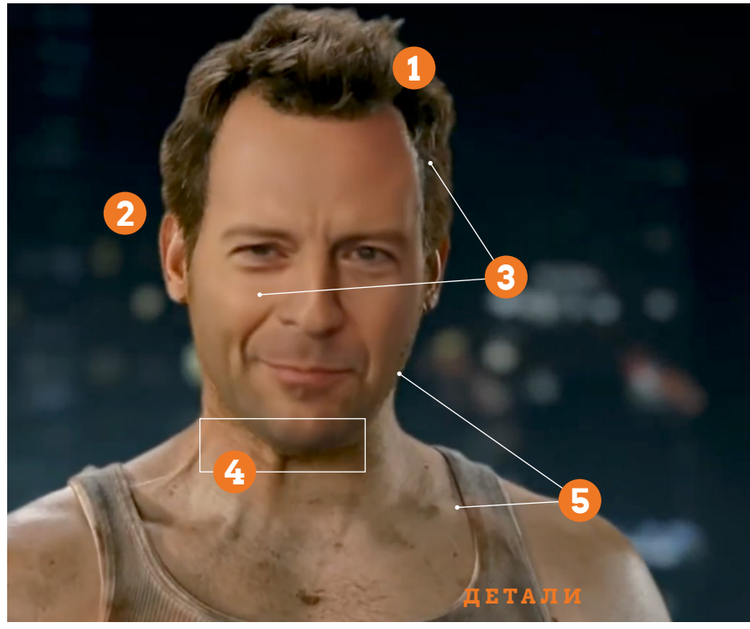
Правила защиты от дипфейков

Дипфейки разнообразны, и технологии очень быстро развиваются. Иногда один дипфейк сочетает несколько техник. Поэтому при проверке контента нужно смотреть на контекст. Так, в видеодипфейках часто освещение лица не совпадает с источником света в помещении. На подделку указывают и технические артефакты: неестественное моргание, несовпадение движения губ и звучащих фраз, странные детали в отражении света, «плывущие» границы изображения, одинаковые движения.

Очень важно следить за своим цифровым следом в Сети: что вы рассказываете в постах, какие фото и видео выкладываете, какой статус ставите в мессенджерах и соцсетях. Для опытных доксеров это кладезь информации. Чтобы им не за что было зацепиться, придерживайтесь правил:

- не публикуйте видео и аудио со своим лицом и голосом в открытых источниках, чатах и мессенджерах;
- сделайте закрытыми профили в соцсетях (доступ только для друзей), незнакомых людей в друзья не добавляйте;
- не публикуйте точную информацию о том, где находитесь и куда собираетесь;
- обязательно сами связывайтесь с человеком, если приходят нетипичные сообщения или звонки от его имени;
- для общения с родственниками и детьми придумайте кодовое слово;
- если вы получили видео- или аудиосообщение с просьбой перевести/занять деньги, обязательно перезвоните сами и лично переговорите с человеком, от которого поступила просьба.

Пример работы дипфейк-алгоритма



Частые признаки дипфейков

1. Размытие на границе наложения (лучше всего заметно на волосах)
2. Неестественно большие или маленькие уши
3. Резкие перепады освещения
4. Разница в цвете на границе наложения
5. Разница в детализации кожи на лице и теле

Как защитить себя при онлайн-покупках

ПОКУПКИ В ИНТЕРНЕТЕ ДАВНО СТАЛИ ЧАСТЬЮ ЦИФРОВОЙ ПОВСЕДНЕВНОСТИ. ВМЕСТЕ С ИХ ПОПУЛЯРНОСТЬЮ **РАСТЕТ ЧИСЛО МОШЕННИЧЕСКИХ СХЕМ — ОТ САЙТОВ-КЛОНОВ ДО ПОДДЕЛЬНЫХ МАГАЗИНОВ И ФАЛЬШИВЫХ СКИДОК.** ПОЭТОМУ ЦИФРОВАЯ БЕЗОПАСНОСТЬ НАЧИНАЕТСЯ НЕ ТОЛЬКО С НАДЕЖНОГО ПАРОЛЯ, НО И С ГРАМОТНОГО ПОВЕДЕНИЯ ПРИ ОНЛАЙН-ПОКУПКАХ. НЕСКОЛЬКО ПРОСТЫХ ПРАВИЛ ПОМОГУТ СДЕЛАТЬ ИХ ДЕЙСТВИТЕЛЬНО БЕЗОПАСНЫМИ.

текст:
Юлия ФАЛЛЕР

Маркетплейс — это не гарантия абсолютной безопасности

Крупные торговые платформы значительно снижают риски, однако полностью их не исключают. Ответственный покупатель всегда проверяет карточку продавца, условия доставки и возврата, а заказ оплачивает исключительно через встроенную систему платежей. После оплаты важно сохранить электронный чек и подтверждение заказа. Эти документы могут стать решающим аргументом при возникновении спора.

Слишком низкая цена — повод насторожиться

Если стоимость товара заметно ниже средней по рынку, внимательно изучите описание, характеристики, отзывы и условия доставки. Сверхвыгодные предложения нередко используются для привлечения покупателей к мошенническим схемам.

Заведите отдельную карту для интернет-покупок

Для онлайн-покупок полезно завести отдельную банковскую карту или отдельный счет. Пополняйте эту карту только непосредственно перед оплатой. Даже если ее данные будут скомпрометированы, злоумышленники не смогут получить доступ к вашим основным средствам.

Если покупаете через сервисы объявлений

На площадках, где продавцы общаются с покупателями напрямую, нужны дополнительные меры предосторожности. Не переводите деньги на личные банковские карты до получения товара, не переходите по сторонним ссылкам и не сообщайте коды подтверждения из СМС или push-уведомлений. Для оплаты используйте только официальные сервисы самой площадки, если они предусмотрены.

Сайты-клоны: когда знакомый магазин оказывается подделкой

Мошенники часто создают сайты, которые выглядят почти так же, как страницы известных интернет-магазинов. Они копируют логотип, дизайн, фотографии товаров и даже акции, поэтому с первого взгляда отличить подделку бывает непросто. Но цель такого сайта не продажа товаров, а кража денег или данных банковской карты. После оплаты покупатель либо вообще не получает заказ, либо его платежные данные оказываются у мошенников.

Чтобы не попасться, всегда обращайте внимание на адрес сайта в браузере. Иногда мошенники меняют всего одну букву или символ: например, вместо официального адреса используют очень похожий. Не переходите в интернет-магазины по ссылкам из сообщений, мессенджеров или сомнительной рекламы. Безопаснее самостоятельно набрать адрес сайта в браузере или воспользоваться официальным приложением магазина. Перед оплатой также убедитесь, что соединение защищено: в адресной строке есть значок замка, а адрес начинается с https://.

Когда исполнитель найден в интернете

Сегодня многие ищут мастеров по ремонту, сантехников, электриков или репетиторов через сервисы объявлений и цифровые платформы. Однако привлекательная цена в объявлении нередко оказывается лишь частью итогового счета. Стоимость выезда, диагностики, расходных материалов или дополнительных работ может выясниться уже после выполнения заказа. Поэтому все условия необходимо согласовывать заранее.

Хорошая практика — получение прайс-листа до начала работ, фиксация договоренностей в переписке и обязательное получение чека после оплаты. Эти простые действия помогают избежать конфликтов и становятся доказательством в случае обращения клиента за защитой своих прав.

Бесплатные предложения бывают слишком дорогими

Особую категорию рисков представляют схемы, основанные не на техническом взломе, а на социальной инженерии. Бесплатные косметические процедуры, массажи, презентации товаров, дегустации или медицинские консультации зачастую становятся лишь первым этапом психологического давления. После демонстрации услуги посетителю начинают настойчиво предлагать дорогостоящие программы, убеждая оформить покупку немедленно, иногда даже в кредит. Формально подобные действия могут не нарушать закон, однако используют хорошо известные психологические приемы воздействия на человека. Если организаторы мероприятия настойчиво требуют взять с собой паспорт или принять решение «здесь и сейчас», лучше отказаться от участия.

«Честный знак»: как проверить товар до покупки

Даже если товар продается на известной площадке, это не гарантирует его подлинность. Одним из инструментов защиты от контрафакта стала государственная система цифровой маркировки «Честный знак». Она охватывает десятки категорий продукции — обувь, одежду, парфюмерию, автомобильные шины, лекарства, молочную продукцию, воду, фотоаппараты, велосипеды и ряд других товаров.

Каждая единица продукции, подлежащая обязательной маркировке, получает уникальный цифровой код Data Matrix. В нем содержится информация о происхождении товара, производителе, дате выпуска и движении продукции по всей цепочке поставок — от предприятия до магазина. Это позволяет сделать оборот товаров более прозрачным и затрудняет продажу контрафактной продукции.

Проверить товар можно самостоятельно с помощью бесплатного приложения «Честный знак». Достаточно отсканировать код маркировки камерой смартфона. Приложение покажет основные сведения о товаре: кто его произвел, легально ли он введен в оборот, соответствует ли маркировка данным государственной системы. Если код отсутствует, не считывается или сведения не совпадают с фактическим товаром, это может свидетельствовать о нарушении правил маркировки или попытке реализации подделки. Использование системы особенно актуально при покупке дорогостоящих товаров, лекарственных препаратов, обуви, одежды и другой продукции, которую чаще всего подделывают.

Если ваши права нарушены

Даже самая тщательная проверка не гарантирует отсутствия проблем. Если продавец нарушил условия сделки, прислал товар ненадлежащего качества или отказался выполнять свои обязательства, важно действовать последовательно.

Первый шаг — направить письменную претензию продавцу. Если договориться не удалось, следует обратиться в Роспотребнадзор. При этом необходимо сохранить все подтверждения покупки: чеки, переписку, фотографии товара и документы об оплате. Именно они становятся основой для защиты прав потребителя. Роспотребнадзор бесплатно помогает в защите прав потребителей, включая судебную защиту. Главное — иметь подтверждающие документы о покупке и качестве товара/услуги.

КОНСУЛЬТАЦИЯ

Консультации по вопросам защиты прав потребителей

- **8 800 100 00 04** — единый консультационный центр Роспотребнадзора
- **8 800 350 41 56** — горячая линия Роспотребнадзора в Томской области

Один пароль на все случаи жизни?

Как не дать мошенникам извлечь выгоду из ваших персональных данных

текст: Юлия ФАЛЛЕР

КАЖДОЕ УТРО НАЧИНАЕТСЯ ОДИНАКОВО: МЫ БЕРЕМ СМАРТФОН, ПРОВЕРЯЕМ СООБЩЕНИЯ, ЗАХОДИМ В ИНТЕРНЕТ-БАНК, ОТКРЫВАЕМ РАБОЧУЮ ПОЧТУ, СОЦИАЛЬНЫЕ СЕТИ, МАРКЕТПЛЕЙСЫ. **ЗА ДЕНЬ МЫ ИСПОЛЬЗУЕМ ДЕСЯТКИ АККАУНТОВ И РЕДКО ЗАДУМЫВАЕМСЯ О ТОМ, ЧТО КАЖДЫЙ ИЗ НИХ — ЭТО ДВЕРЬ В НАШУ ЦИФРОВУЮ ЖИЗНЬ.** И ЕСЛИ ЭТА ДВЕРЬ ЗАКРЫТА НА СЛАБЫЙ ЗАМОК, ОТКРЫТЬ ЕЕ МОШЕННИКАМ НЕ СОСТАВИТ ТРУДА.

По данным специалистов по кибербезопасности, одной из самых распространенных ошибок пользователей остается простой пароль. «1234», «1111», «qwerty», имя домашнего питомца или дата рождения — подобные комбинации до сих пор встречаются очень часто. Они удобны, легко запоминаются, но легко подбираются специальными программами, которыми пользуются злоумышленники.

Еще опаснее привычка использовать один и тот же пароль для всех сервисов. Представьте, что вы потеряли ключ от квартиры, а он одновременно подходит к машине, даче, офису и банковской ячейке. Стоит одному сайту столкнуться с утечкой данных — и злоумышленники получают возможность попробовать этот же пароль на электронной почте, в интернет-банке, социальных сетях и других сервисах. Да, запомнить несколько десятков сложных комбинаций практически невозможно. Но и для этой проблемы уже давно есть удобное решение.

Почему менеджер паролей — это хороший помощник

Многие продолжают хранить пароли в заметках телефона, записывать их в блокнот или вовсе надеются на память. Но все эти способы имеют серьезные недостатки. Сегодня специалисты рекомендуют использовать менеджеры паролей — специальные приложения, которые надежно хранят все учетные данные в зашифрованном виде. Пользователю достаточно помнить только один мастер-пароль, открывающий доступ ко всему хранилищу.

Такие программы не только хранят пароли, но и умеют создавать действительно сложные комбинации буквально одним нажатием кнопки. Более того, менеджер автоматически подставляет учетные данные только на настоящий сайт. Если пользователь случайно попадет на поддельную страницу, имитирующую известный сервис, программа просто не предложит сохраненный пароль. Это помогает защититься от одной из самых популярных схем интернет-мошенничества — фишинга.

Что такое токены и почему пароль все чаще не покидает ваше устройство

Сегодня многие сервисы постепенно переходят на более безопасные способы авторизации. Вместо постоянной передачи пароля используются специальные цифровые токены или так называемые ключи доступа (Passkeys). Простыми словами можно объяснить так: после успешного входа сервис выдает устройству специальный цифровой «пропуск» — токен. При последующих обращениях токен подтверждает, что на ресурс заходит действительно авторизованный пользователь. Сам пароль при этом не передается каждый раз через интернет, а значит, его сложнее перехватить.

Еще более безопасная технология — ключи доступа (Passkeys). Они используют криптографические ключи, которые хранятся на устройстве пользователя и подтверждаются отпечатком пальца, Face ID или ПИН-кодом устройства. Даже если злоумышленник создаст поддельный сайт, украсть такой ключ практически невозможно — он просто не подойдет для другого ресурса. Если сервис предлагает применять Passkeys или вход без пароля, специалисты рекомендуют пользоваться этой возможностью.

Второй замок для вашего аккаунта

Даже самый сложный пароль нельзя считать абсолютной гарантией безопасности. Иногда злоумышленники получают доступ к базам данных компаний или пытаются обманом узнать пароль у самого пользователя. Именно поэтому все больше интернет-сервисов предлагают включить двухфакторную аутентификацию. Звучит сложно, но работает очень просто. После ввода логина и пароля система просит подтвердить вход дополнительным способом — например, ввести код из СМС, push-уведомления или специального приложения. Даже если кто-то узнает ваш пароль, войти в аккаунт без второго подтверждения он уже не сможет. А если код неожиданно приходит вам без попытки входа с вашей стороны, это повод насторожиться. Скорее всего, кто-то пытается получить доступ к вашему аккаунту. В такой ситуации пароль необходимо сменить как можно быстрее.

Как чаще всего теряют аккаунты

Многие уверены, что аккаунты взламывают исключительно сложными хакерскими атаками. Но на практике злоумышленники чаще используют человеческую невнимательность. Например, пользователь получает сообщение якобы от службы поддержки социальной сети с просьбой подтвердить аккаунт по ссылке. Страница выглядит почти как настоящая, человек вводит логин, пароль и код подтверждения — и передает их мошенникам.

Другая распространенная схема связана с игровыми аккаунтами. Владельцу обещают бесплатную игровую валюту, редкий предмет или участие в закрытом тестировании новой версии игры. Для этого предлагают войти через специальный сайт. После ввода данных пользователем злоумышленники получают полный контроль над аккаунтом, а затем перепродают его вместе с накопленными достижениями, персонажами и внутриигровыми покупками.

Не менее часто похищают аккаунты в социальных сетях. Получив доступ к странице, мошенники начинают рассылать сообщения друзьям владельца с просьбой срочно перевести деньги или переходят к вымогательству, требуя оплату за возврат доступа.

Как снизить риск потери аккаунта

Защита аккаунта — это не только надежный пароль. Важно заранее подготовиться к ситуации, если злоумышленники попытаются получить доступ. Специалисты рекомендуют соблюдать несколько простых правил:

- использовать уникальные пароли для каждого сервиса;
- хранить их в менеджере паролей, а не в заметках или мессенджерах;
- включить двухфакторную аутентификацию, а где возможно — использовать Passkeys;
- проверить и регулярно обновлять резервную электронную почту и номер телефона для восстановления доступа;
- хранить резервные коды восстановления в надежном месте — они помогут вернуть доступ, если телефон будет утерян;
- не сообщать никому коды подтверждения, даже если собеседник представляется сотрудником банка, службы поддержки или правоохранительных органов;
- периодически проверять список устройств, с которых выполнен вход в аккаунт, и завершать неизвестные сеансы.

t2bgao-fuwzUj-qikvyq

ВАЖНО

Хороший пароль — это не случайность

Надежный пароль сегодня — обязательный элемент цифровой гигиены. Специалисты рекомендуют использовать комбинации длиной не менее 10—12 символов. Лучше, если в них будут присутствовать заглавные и строчные буквы, цифры и специальные символы.

При этом пароль не должен иметь ничего общего с владельцем. Даты рождения детей, номера телефонов, имена супругов, любимых футбольных команд и клички домашних животных легко находятся в социальных сетях и становятся первыми вариантами для подбора.

текст:
Юлия СОЛОВЕЙ

Биометрические данные: что это такое и могут ли их украсть мошенники

КОГДА В РОССИИ ВВЕЛИ ВОЗМОЖНОСТЬ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ПО БИОМЕТРИЧЕСКИМ ДАННЫМ, БУМА СДАЧИ БИОМЕТРИИ НЕ СЛУЧИЛОСЬ. ЛЮДИ БОЯТСЯ, ЧТО И ЭТА ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ БУДЕТ СКОМПРОМЕТИРОВАНА. ОДНАКО **БИОМЕТРИЯ СЕГОДНЯ НЕ ТОЛЬКО ЗАМЕНЯЕТ ПАСПОРТ, НО ДАЕТ ВОЗМОЖНОСТЬ ПОЛУЧАТЬ УДАЛЕННО МНОГИЕ УСЛУГИ, В ТОМ ЧИСЛЕ ФИНАНСОВЫЕ.** РАЗОБРАЛИСЬ, ЧТО ТАКОЕ БИОМЕТРИЧЕСКИЕ ДАННЫЕ, КАКИЕ ПЛЮСЫ ОНИ ДАЮТ И ПОЧЕМУ НЕ СТОИТ БОЯТЬСЯ СДАВАТЬ БИОМЕТРИЮ.

Что такое биометрия и где она хранится

Биометрия — это уникальные физические данные конкретного человека, которые не встречаются больше ни у кого, — радужка глаз, папиллярные узоры на ладонях и пальцах, рисунок вен, голос. Если бумажный документ можно подделать, то биометрические данные нет. Это на сто процентов надежный идентификатор личности.

Биометрические данные не хранятся в их первоначальной форме. Это значит, что в базе биометрических данных не получится найти некую папку, подписанную именем человека, в которой лежит звуковой файл с его голосом и снимок лица или радужки глаз. Биометрические данные хранятся в ЕБС (Единая биометрическая система), а персональные данные из документов — в другой системе. Это две независимые базы данных, а связь между ними можно установить, имея уникальный идентификатор, который может получить только сертифицированная организация.

Кроме того, биометрические данные поступают и хранятся в ЕБС в виде цифрового кода. База биометрии надежно защищена от взлома. Но даже если взломщик получит к ней доступ, он найдет только цифровые коды, которые невозможно соотнести с конкретными людьми.

Как работает идентификация по биометрии

Как правило, для идентификации используется голос, слепок лица, радужка глаз и отпечатки пальцев. Самый простой пример биометрической идентификации — разблокировка смартфона через распознавание лица.

Для включения этой функции пользователю предлагается посмотреть в камеру, устройство сканирует лицо, считывает важные параметры и запоминает их. Когда пользователь захочет разблокировать смартфон и посмотрит в камеру, она вновь просканирует лицо, устройство соотнесет изображение с тем, что хранится в памяти. Если данные совпали, происходит разблокировка. Так же происходит идентификация по голосу, отпечатку пальца или радужке глаза.

Как сдать свою биометрию в ЕБС

Способ ее регистрации зависит от целей человека. Для максимальных возможностей нужна подтвержденная биометрия, с которой можно открывать вклады в банках, брать кредит или выпустить бесплатно усиленную квалифицированную электронную подпись (УКЭП). Для оплаты покупок в пределах определенной суммы или для входа в личный кабинет на «Госуслугах» достаточно стандартной и упрощенной биометрии.

Подтвержденную биометрию можно сдать только лично в уполномоченном банке, а упрощенную и стандартную — прямо из дома при наличии смартфона с приложением «Госуслуги Биометрия». Для стандартной биометрии нужен смартфон с NFC-модулем и загранпаспорт нового образца.

Какие преимущества дает биометрия

Биометрические данные, зарегистрированные в ЕБС, позволяют дистанционно получать финансовые услуги. Например, можно не выходя из дома оформить кредит или открыть вклад в банке, у которого нет отделения в вашем городе, но который предлагает выгодные условия. Или оплатить покупку улыбкой, если вдруг забыли карту дома. Появляются и банкоматы, где не требуется карта, — можно снять деньги, пройдя идентификацию по биометрии.

Биометрия используется не только для непосредственной идентификации человека, но и считается самым безопасным фактором для двухфакторной аутентификации. Если СМС с кодом подтверждения, например, можно перехватить, то с голосом или слепком лица это не получится сделать.

Насколько это безопасно

Организации, уполномоченные собирать биометрические данные, не вправе хранить их у себя. После регистрации биометрия сразу в зашифрованном виде передается в Единую биометрическую систему и там хранится под надежной защитой. Биометрические данные человека обезличены, так как его персональные данные хранятся в другой базе.

Установить соответствие между данными этих двух баз нельзя без уникального идентификатора. Только он может связать цифровые коды, в которых зашифрованы слепок лица и образец голоса, с персональными данными определенного человека. Поэтому опасаться за утечку или кражу биометрии не стоит. Без идентификатора эти данные похожи на замок без ключа и бесполезны для мошенника.

Не получится у мошенников пройти идентификацию по биометрии от имени другого человека, создав дипфейк: система распознавания проверяет изображение с помощью ИИ на предмет подделки. К тому же идентификация происходит по двум параметрам — изображению и голосу.

Существует миф о том, что мошенники незаметно фотографируют людей или записывают их голос, чтобы получить их биометрические данные. Но и это только миф: камера смартфона не подходит для этих целей, нужны строгие настройки ракурса и освещения, чтобы снимок или запись можно было использовать в качестве биометрии для идентификации.

Можно ли отозвать свою биометрию

Сдача и использование биометрии — добровольное решение человека. Он может в любое время удалить свои данные из ЕБС через «Госуслуги» (во вкладке «Биометрия»).

СПРАВКА

Что «умеет» биометрия

Подтвержденная (действует 5 лет)

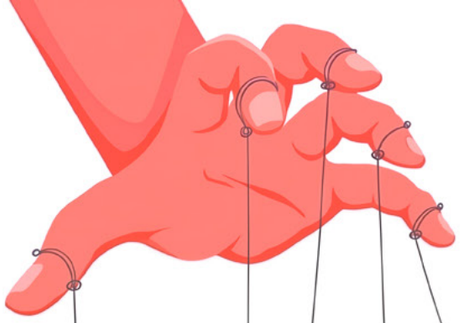
- Оплата товаров и услуг в пределах 5 000 ₽;
- Оплата проезда в транспорте;
- Проход на территорию госорганов и организаций;
- Безопасная авторизация на «Госуслугах»;
- Дистанционное заключение договоров на оказание услуг связи;
- Дистанционное оформление карты болельщика;
- Дистанционная сдача промежуточной и итоговой аттестации в вузах;
- Получение услуг, требующих идентификации по паспорту;
- Выпуск УКЭП.

Стандартная (5 лет)

- Оплата товаров и услуг в пределах 5 000 ₽;
- Оплата проезда в транспорте;
- Проход на территорию госорганов и организаций;
- Безопасная авторизация на «Госуслугах»;
- Дистанционное заключение договоров на оказание услуг связи;
- Дистанционное оформление карты болельщика;
- Дистанционная сдача промежуточной и итоговой аттестации в вузах.

Упрощенная (3 года)

- Оплата товаров и услуг в пределах 2 500 ₽;
- Оплата проезда в транспорте;
- Проход на территорию госорганов и организаций;
- Получение услуг в организации, которая зарегистрировала биометрию.



Дропы

ЧТОБЫ ОСТАТЬСЯ В ТЕНИ, МОШЕННИКИ НИКОГДА НЕ ИСПОЛЬЗУЮТ ДЛЯ ПОЛУЧЕНИЯ ДЕНЕГ ОТ ЖЕРТВ СВОИ БАНКОВСКИЕ КАРТЫ. ДЛЯ ЭТОГО ПРИВЛЕКАЕТСЯ АРМИЯ ПОСРЕДНИКОВ — ДРОПОВ. ИМЕННО ИХ ПЕРВЫМ ДЕЛОМ ВЫЧИСЛЯЕТ ПОЛИЦИЯ, РАСПУТЫВАЯ ЦЕПОЧКУ ПЕРЕВОДОВ ОТ ЖЕРТВ ОБМАНА. А ДАЛЬШЕ — УГОЛОВНОЕ ДЕЛО, КОТОРОЕ МОЖЕТ ЗАКОНЧИТЬСЯ РЕАЛЬНЫМ СРОКОМ. ПОЧЕМУ И КАК ЛЮДИ СТАНОВЯТСЯ ДРОПАМИ, КАКОВА ОТВЕТСТВЕННОСТЬ ЗА ЭТО И КАК ПОНЯТЬ, ЧТО ВАС ПЫТАЮТСЯ ВТЯНУТЬ В ДРОПЕРСТВО?

Как вместо денег люди зарабатывают тюремный срок

текст:
Оксана КУДРЯВЦЕВА,
Юлия СОЛОВЕЙ

Кто такие дропы и как ими становятся

С английского глагол *drop* переводится как *капать, сливать, бросать*. Действительно, дропы получают небольшие суммы, а затем перекидывают их на другой счет, который укажут им мошенники. Мелкими суммами деньги через цепочку посредников стекаются к организатору схемы, вычислить которого очень сложно из-за запутанной траектории переводов.

Дропами становятся по-разному. Кто-то вовлекается случайно и даже не подозревает, что его втянули в мошенническую схему, попросив вернуть «ошибочный перевод» на карту. Таких дропов называют разводными, потому что их привлекли обманом, развели. Другая категория — неразводные дропы: они прекрасно знают, чем занимаются, вдобавок могут еще и вербовать новых посредников, получая с этого доход.

Как мошенники находят дропов

Чаще всего преступники маскируются под работодателей и менеджеров по персоналу. Через фейковые аккаунты размещают в интернете объявления о несложной работе, не требующей опыта, и при этом с гибким графиком и быстрой оплатой. Такие объявления легко цепляют школьников и студентов: у них нет опыта, но есть желание получить легкие деньги и стать финансово независимыми. Поэтому молодежь — основной контингент, среди которого злоумышленники ищут дропов, что доказывает статистика: средний возраст дропа — от 14 лет до 21 года.

Мошенники предлагают выполнить простые задачи: забрать посылку, оформить банковскую карту, передать реквизиты, провести деньги через счет, оставив определенную сумму себе в качестве вознаграждения. Подросток думает, что работает администратором лотерей, как было написано в объявлении о вакансии, но на самом деле переводит не выигрыши участникам, а украденные деньги другим дропам.

Работа дропа — это не всегда перевод денег. Мошенники могут за вознаграждение попросить подростка оформить банковскую карту или новую сим-карту и передать им. Потом жулики используют это для отмывания денег. Однако после введения запрета на выдачу банковских карт несовершеннолетним без письменного разрешения родителей злоумышленникам будет гораздо сложнее использовать эту схему.

Еще один способ вербовки дропов — социальная инженерия. Например, вы снимаете деньги в банкомате, и тут к вам подходит приличный с виду человек с просьбой о помощи. Якобы он ждет перевод от родственника, а карту найти не может. Просит дать номер вашей карты, чтобы деньги прислали на нее, а вы бы их сняли и передали просителю. В роли родственника, конечно же, дроп, которому нужно «скинуть» сумму дальше. Если согласитесь, то обналичите через свою карту мошеннический заработок. Схема с «ошибочным» переводом тоже из области социальной инженерии. Если отказаться возвращать перевод на указанную мошенником карту, то его просьба превращается в требование, начинается давление, угрозы в расчете на то, что человек испугается, не захочет связываться и все же переведет деньги.

Злоумышленники используют для отмывания денег не только чужие карты, но и аккаунты в онлайн-банке или на маркетплейсе. Если вам предлагают деньги в обмен на передачу аккаунта, вас хотят втянуть в мошенническую схему в качестве дропа.

Наказание за участие в дроперских схемах

Выполнение операций с деньгами, добытыми путем мошенничества, закон считает преступлением. При этом незнание об участии в дроперстве не освобождает от ответственности перед законом. В зависимости от степени вовлеченности в мошенническую схему дропам может грозить административный штраф или уголовная ответственность: принудительные работы или же ограничение/лишение свободы. Так, за передачу своих реквизитов и проведение финансовых операций по указанию третьих лиц суд может назначить до 3 лет колонии и штраф 100—300 тыс. руб. За продажу чужих реквизитов грозит до 6 лет колонии и штраф 300 тыс.—1 млн руб.

Вдобавок к наказанию дропы попадают в базу ФинЦЕРТ — это реестр Центрального банка, куда

ДЕТАЛИ

Специализация дропов

Заливщик вносит на свой счет в банке полученные от мошенника наличные и затем переводит другим дропам.

Транзитник принимает на свою карту переводы и перечисляет их на другие карты либо электронный кошелек за процент от суммы.

Обнальщик снимает с карты поступившие деньги, часть забирает как плату за свои услуги, остальное передает курьеру.

Универсал может выполнять все дроперские функции — заливать наличные, переводить дальше или обналичивать переводы.

вносятся данные россиян, чьи транзакции по карте имеют признаки мошенничества. Участникам этого списка банки блокируют карты, делая невозможным использование онлайн-банка и банковских приложений. Если человек внесен в базу ФинЦЕРТ, но без блокировки карты, то ему ограничиваются переводы: в месяц нельзя перевести ни себе, ни другим людям больше 100 000 руб.

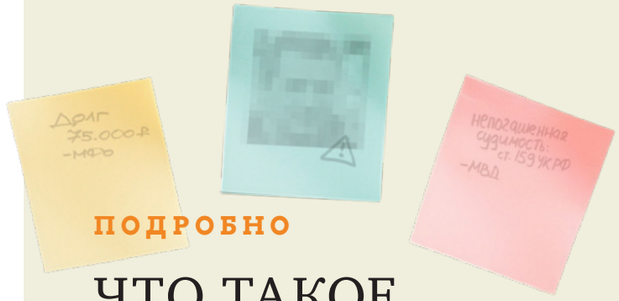
Что делать, чтобы случайно не стать дропом

Во-первых, нужно быть «в теме»: интересоваться, какие схемы используют мошенники и как им противостоять. Во-вторых, беречь свою банковскую карту: никому не передавать ни ее саму, ни реквизиты. И не соглашаться выполнять операции с деньгами по просьбе незнакомых людей. А если просит знакомый, но просьба вам кажется странной, откажите: уж лучше испортить отношения с человеком, чем потерять свободу.

Ошибочные переводы от третьих лиц возвращайте только через банк путем отмены транзакции. Обо всех подозрительных операциях по карте и звонках сообщайте в ЦБ или полицию.

Если по незнанию выполнили перевод по просьбе мошенника, а уже позже поняли, что стали дропом, примите меры:

- Заблокируйте карту, с которой переводились деньги. На звонки и сообщения мошенников не отвечайте.
- Сделайте скрины чата с мошенниками и истории звонков, чтобы зафиксировать номер, с которого они звонили.
- Позвоните на горячую линию вашего банка и объясните ситуацию, узнайте, не зафиксировал ли банк подозрительные операции по вашей карте.
- Обратитесь в полицию и расскажите, что случайно стали дропом, сообщите все, что вам известно об использовании вашей карты мошенниками.



ПОДРОБНО

ЧТО ТАКОЕ БАЗА ФИНЦЕРТ И КТО МОЖЕТ ОКАЗАТЬСЯ В НЕЙ

ФинЦЕРТ — это структурное подразделение Банка России, занимающееся кибербезопасностью. На его базе создана система обмена данными в сфере финбезопасности, к которой могут подключиться финансовые организации, правоохранительные структуры, интернет-провайдеры, сотовые операторы и другие организации, заинтересованные в противодействии мошенничеству. Участники системы могут оперативно отправить в ЦБ данные о мошеннических операциях, атаках взломщиков, переводах денег без согласия клиентов банков и проч.

Также на базе ФинЦЕРТ ведется реестр лиц, замеченных в проведении подозрительных финансовых операций — так называемый «черный список ЦБ». Попасть в него может клиент банка, по счету которого зафиксированы транзакции, связанные с фишингом, отмыванием или обналичиванием денег. Если информацию о таких операциях в ЦБ передал банк, то клиенту ограничивают сумму переводов: в месяц не более 100 000 рублей. себе и другим людям. Если данные о человеке поступили из МВД, ему заблокируют карты, доступ в онлайн-банк и банковские приложения. Ограничения действуют до момента исключения из базы.

В декабре 2025 года Центробанк в сотрудничестве с МВД запустил процедуру реабилитации для участников черного списка. Теперь они вправе запросить информацию о транзакции, из-за которой в него попали (речь идет о возврате суммы, зачисленной клиенту жертвой мошенника), а затем обратиться в банк отправителя и отменить операцию. Информация о возврате денег пострадавшему передается банком в ЦБ. На этом основании регулятор примет решение о реабилитации, то есть об исключении человека из реестра мошенников.

Самозапреты

Как не дать мошенникам извлечь выгоду из ваших персональных данных

текст:
Юлия СОЛОВЕЙ

ОНЛАЙН-СЕРВИСЫ ОЩУТИМО ОБЛЕГЧАЮТ НАМ ЖИЗНЬ И ЭКОНОМЯТ ВРЕМЯ. А С ДРУГОЙ СТОРОНЫ ДЕЛАЮТ НАС УЯЗВИМЫМИ, ПОСКОЛЬКУ ОБРАБАТЫВАЮТ НАШИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ. ПОЛУЧИВ ДОСТУП К ДАННЫМ ДРУГОГО ЧЕЛОВЕКА, МОШЕННИКИ МОГУТ ОФОРМИТЬ НА НЕГО КРЕДИТ, СИМ-КАРТУ ИЛИ ПРОДАТЬ ЕГО НЕДВИЖИМОСТЬ. НО **ДАЖЕ ЕСЛИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ УЖЕ СКОМПРОМЕТИРОВАНЫ, ЧЕРЕЗ УСТАНОВКУ САМОЗАПРЕТОВ МОЖНО СДЕЛАТЬ ТАК, ЧТО ЖУЛИКИ НЕ СМОГУТ ДОСТИЧЬ СВОИХ ЦЕЛЕЙ.** РАССКАЗЫВАЕМ, ЧТО ТАКОЕ САМОЗАПРЕТ, В КАКИХ СФЕРАХ ИСПОЛЬЗУЕТСЯ И КАК ЕГО УСТАНОВИТЬ.

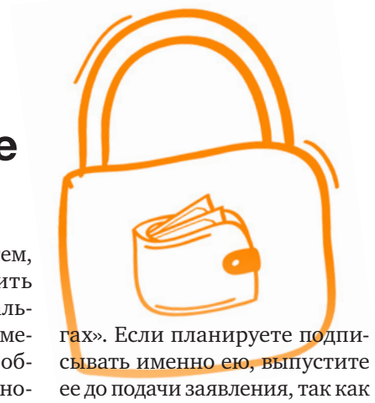
Что такое самозапрет и как он работает

Самозапрет — это добровольный отказ человека от совершения определенных действий. На сегодняшний день можно запретить себе оформление кредитов, заключение договоров на услуги связи и сделки с недвижимостью.

Принцип действия любого самозапрета сводится к невозможности получить услугу до тех пор, пока запрет не снят. Ограничения закрывают путь мошенникам, а когда речь идет о кредитах, помогают людям избежать импульсивных покупок на заемные деньги. Установить и снять самозапреты можно через портал «Госуслуги» или лично в офисе МФЦ.

Принцип действия любого самозапрета сводится к невозможности получить услугу до тех пор, пока запрет не снят.

Самозапрет на получение кредитов



Мошенники пользовались тем, что займы можно оформить онлайн. Похищали персональные данные людей и от их имени брали кредиты. Жертва обмана узнавала о задолженности от судебных приставов или коллекторов. Для борьбы с мошенническими займами и был введен самозапрет на кредитование. С его помощью можно полностью или частично запретить себе оформление беззалоговых кредитов. При полном запрете кредит нельзя будет оформить ни лично, ни онлайн, ни по телефону ни в одной кредитной организации. Частичный запрет избирателен: можно запретить кредитование только в МФО или только в банке. Или сделать невозможным определенный способ оформления кредита — например, онлайн-займы.

Установить запрет можно через «Госуслуги» при наличии подтвержденной учетной записи. После авторизации наберите в строке поиска «самозапрет на кредиты». Выберите «Установление запрета» — «Установить запрет» и следуйте инструкциям портала. В конце заявление нужно будет подписать электронной подписью. Простую электронную подпись можно выпустить прямо на «Госуслугах». Если планируете подписывать именно ею, выпустите ее до подачи заявления, так как генерация подписи не мгновенная. Для подписания усиленной подписью понадобится приложение «Госключ».

После подписания документов в разделе «Заявления» на «Госуслугах» появится заявление на установку самозапрета. Внутри него будут файлы pdf — уведомления о том, что в кредитной истории пользователя появится отметка о замозапрете кредитования. Количество уведомлений соответствует количеству бюро кредитных историй (БКИ), в которых хранится кредитное досье человека. На обработку заявления отводится 2 дня. Как только его примут, пользователь получит уведомление об этом, а на следующий день запрет вступит в силу.

Теперь в кредитной истории человека есть отметка о действующем самозапрете, поэтому ни один кредитор не вправе выдать заем такому клиенту. Кредитор, одобривший кредит, не удостоверившись в наличии самозапрета у заемщика, не сможет потребовать от него возврата долга.

Самозапрет на заключение договоров связи

Номер телефона — ключ ко многим сервисам и возможностям. Он нужен для авторизации в онлайн-банке, для создания аккаунта в мессенджере, с его помощью можно подтвердить оформление онлайн-кредита и войти на «Госуслуги». Поэтому мошенники «угоняли» чужие сим-карты или оформляли новые на других людей, чтобы затем использовать их в схемах обмана, оставаясь при этом в тени. Самый простой способ защиты — самозапрет на заключение новых договоров связи. Если его установить, никто не сможет купить на имя человека новую сим-карту, даже он сам. В салоне связи сначала сделают запрос о наличии самозапрета, если он есть, заключение нового договора будет невозможно.

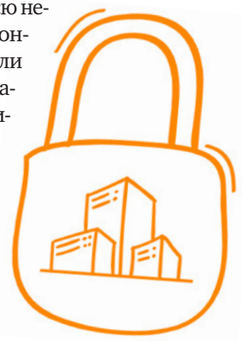
Установить самозапрет на новые сим-карты проще и быстрее через «Госуслуги». В профиле выберите «Сим-карты» — «Запрет на оформление договоров связи» — «Установить». Через несколько минут запрет уже будет действовать. Для установки через МФЦ понадобится время на посещение центра, паспорт и СНИЛС. Снимается запрет только лично в МФЦ. На «Госуслугах» возможность снятия отсутствует: так мошенники не смогут отключить самозапрет, получив доступ к чужому аккаунту, или обманом убедить самого пользователя сделать это.

Но даже если не планируете запрещать себе оформление новых сим-карт, зайдите на «Госуслуги» и проверьте, какие сотовые номера за вами числятся. Так вы убедитесь, что на вас не оформили сим-карту мошенники. После авторизации откройте свой профиль и выберите раздел «Сим-карты». Если обнаружите номер, который не оформляли, заблокируйте его: кликните по номеру, откройте меню «Действия» и выберите «Заблокировать номер». Это временная мера, чтобы «списать» с себя номер, нужно расторгнуть договор с оператором. При наличии усиленной квалифицированной электронной подписи можно сделать это через «Госуслуги». Если ее нет, договор расторгается в офисе оператора по паспорту. Следующий шаг — обращение в полицию и Роскомнадзор. В полицию нужно заявить о факте незаконного оформления сим-карты, а в Роскомнадзор сообщить о нарушении закона «О персональных данных».

И еще: если номером, оформленным на вас, пользовались мошенники, запросите кредитную историю (чтобы узнать, не взяли ли на вас кредит), смените пароли в банковских приложениях и онлайн-банке.

Самозапрет на сделки с недвижимостью

Запрет на продажу недвижимости без личного присутствия собственника — это мера противодействия мошенникам, которые подделывают или добывают обманным путем доверенности. Особенно легко поддаются обману пожилые собственники. Запрет оформляется не на всю недвижимость, а на конкретную квартиру или дом, информация о запрете вносится в Единый государственный реестр недвижимости (ЕГРН). Если при проверке Росреестр видит отметку о запрете, сделка не регистрируется, то есть право собственности не переходит к покупателю. Запрет распространяется не только на продажу объекта недвижимости, его также нельзя подарить, сдать в аренду, оформить пожизненную ренту и сделать предметом залога. Действует запрет до тех пор, пока собственник не снимет его.



Установить запрет можно через «Госуслуги», в личном кабинете на сайте Росреестра или в МФЦ. Для установки запрета онлайн нужно приложение «Госключ» и усиленная квалифицированная электронная подпись.

- **«Госуслуги»:** «Услуги» — «Земля» — «Дом» — «Запрет на действия с недвижимостью без личного участия».
- **Сайт Росреестра:** «Мои услуги и сервисы» — «Иное» — «Внесение записей о невозможности государственной регистрации права без личного участия правообладателя».
- **МФЦ:** для установки запрета через МФЦ нужен паспорт, ИНН и документы на недвижимость.

Независимо от способа установки запрета запись о нем в ЕГРН появится в течение пяти рабочих дней после отправки заявления. Снять запрет может только сам собственник. Без его воли и участия запрет может быть снят в нескольких случаях:

- суд взыскивает недвижимость для погашения ипотечной задолженности;
- недвижимость изымается государством;
- недвижимость подлежит разделу;
- наследник недвижимости хочет переоформить ее на себя;
- на недвижимость наложен арест в рамках уголовного дела.

КСТАТИ

Запрет на массовые обзвоны

Этот запрет не относится к самозапретам, но помогает отсеять телефонный спам и снизить уровень стресса.

Массовый автоматизированный обзвон — это обзвон большого числа людей по базе телефонных номеров через специальную программу. Обычно они проводятся для опроса, рекламы, информирования клиентов. Так делают банки, медицинские клиники, сотовые операторы и другие организации. С 1 сентября 2025 года абоненты могут установить запрет на такие звонки, а операторы обязаны блокировать их.

Включить запрет можно в офисе сотового оператора, в личном кабинете на его сайте или в приложении. Как правило, опция блокировки автоматизированных звонков находится в разделе «Безопасность», «Защита от спама» и т. п. Со следующего дня оператор должен блокировать автоматические звонки на номер абонента. Снять запрет можно в любое время.

Нюанс: запрет на автоматические обзвоны может заблокировать и важные для абонента звонки. Например, медицинская клиника не сможет позвонить ему для подтверждения записи на прием или для информирования об изменениях в работе.

На карту пришли деньги от незнакомца?

Не спешите радоваться — это может обернуться большими проблемами

НЕОЖИДАННЫЙ ПЕРЕВОД ОТ НЕИЗВЕСТНОГО ЧЕЛОВЕКА КАЖЕТСЯ ПРИЯТНОЙ СЛУЧАЙНОСТЬЮ ИЛИ ЧЬЕЙ-ТО ОШИБКОЙ. НО **ИНОГДА ЗА ТАКИМИ ПОСТУПЛЕНИЯМИ СТОЯТ МОШЕННИЧЕСКИЕ СХЕМЫ,** ИЗ-ЗА КОТОРЫХ МОЖНО НЕ ТОЛЬКО ПОТЕРЯТЬ ДЕНЬГИ, НО И ПОПАСТЬ В НЕПРИЯТНУЮ ИСТОРИЮ С БАНКОМ ИЛИ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ. РАССКАЗЫВАЕМ, ЧТО ДЕЛАТЬ, ЕСЛИ НА КАРТУ ПРИШЛИ ЧУЖИЕ ДЕНЬГИ И ИХ ТРЕБУЮТ ВЕРНУТЬ.

текст: Юлия ФАЛЛЕР

Ошибочный перевод: где скрывается риск?

Ошибочные переводы действительно случаются, отправитель может неверно указать номер телефона или карты, и деньги поступят другому человеку. Но даже в такой ситуации не стоит самостоятельно переводить средства обратно по реквизитам, которые сообщает неизвестный отправитель. Это может обернуться неприятностями. Самая малая — потеря собственных денег.

Одна из распространенных схем выглядит так: мошенники подделывают сообщения о зачислении средств, используя технологии подмены данных отправителя. Человек получает уведомление о переводе, которого на самом деле не было, а затем ему звонят или пишут с просьбой вернуть деньги. Если не догадаться проверить баланс и историю операций, можно отправить злоумышленникам собственные средства.

Существуют и более сложные сценарии. Например, деньги действительно поступают на счет, после чего отправитель просит вернуть их на другие реквизиты. Получатель выполняет просьбу, а позже выясняется, что первоначальный перевод связан со спорной или мошеннической операцией. В результате возникают финансовые и юридические риски, а разбираться в ситуации приходится уже получателю средств. Похожий механизм используется в схемах с поддельными интернет-магазинами. Покупателя привлекают необычно низкими ценами, он оплачивает товар, а деньги поступают на счет постороннего человека. Затем мошенник связывается с владельцем счета и просит вернуть «ошибочный перевод» на другие реквизиты. Так злоумышленник получает деньги, покупатель остается без товара, а к владельцу счета могут возникнуть вопросы о происхождении и дальнейшем движении средств.

Особую опасность представляют схемы с использованием дропов — посредников, через счета которых проходят деньги, полученные преступным путем. Для злоумышленников это способ скрыть следы и затруднить расследование. Один из способов вовлечь человека в такую цепочку — перевести ему деньги и попросить отправить их дальше на другой счет. Даже если человек не подозревал о происхождении средств, участие в подобных операциях может привлечь внимание банка и правоохранительных органов. Ситуация становится еще более рискованной, если за перевод предлагают вознаграждение или процент от суммы. Поэтому любые просьбы переслать деньги незнакомым людям следует рассматривать как потенциально опасные.

На карту пришли деньги от неизвестного. Что делать?

Первое — убедиться, что деньги действительно поступили на счет. Проверять нужно не сообщение или СМС, а баланс и историю операций в мобильном приложении банка или интернет-банке. Если зачисления нет, скорее всего вас пытаются обмануть жулики.

Иногда цель злоумышленников — не только деньги. В сообщении они могут прислать ссылку якобы для отмены операции или уточнения деталей перевода. Такие ссылки ведут на фишинговые сайты, где пользователя просят ввести данные карты, коды подтверждения или логин и пароль от интернет-банка. Передача этих сведений открывает мошенникам доступ к счету.

Если деньги действительно поступили от неизвестного отправителя и с вами связываются по поводу возврата, не стоит вступать в спор или переводить средства самостоятельно. Сообщите, что готовы урегулировать ситуацию через банк, и обратитесь в службу поддержки своей кредитной организации. Банк подскажет порядок действий и зафиксирует обращение. Можно предложить и самому отправителю обратиться в свой банк для урегулирования вопроса.

Если речь действительно идет об ошибке, такой порядок обычно не вызывает возражений. Мошенники же нередко начинают торопить, давить на жалость или угрожать последствиями, требуя немедленного перевода денег на указанные ими реквизиты.

А если неизвестный человек настойчиво звонит, пишет сообщения или угрожает, имеет смысл обратиться в полицию. Сохраните переписку, сделайте скриншоты сообщений, а при возможности запишите телефонные разговоры. Эти материалы могут пригодиться при разбирательстве.

ИНСТРУКЦИЯ

Как действовать при получении перевода от неизвестного

1 Проверьте факт зачисления денег
Сделать это можно через приложение банка или интернет-банк.

2 Не доверяйте сообщениям
Если перевода нет, игнорируйте просьбы о возврате. Не переходите по ссылкам и не сообщайте данные карты, коды из СМС или пароли.

3 Обратитесь в банк
Если деньги поступили, сообщите об этом в службу поддержки по телефону или через чат с банком. Оставьте заявление на отмену ошибочного перевода, даже если никто не требовал вернуть деньги.

Закон расценивает невозврат денег как необоснованное обогащение. Если уже получили звонок или сообщение с просьбой о возврате денег, сделайте скриншоты и прикрепите к сообщению в чате с банком.

4 Не пользуйтесь чужими деньгами
До выяснения обстоятельств не тратьте поступившие средства и не переводите их на другие счета.

5 Фиксируйте переписку
При навязчивых требованиях вернуть деньги, угрозах или попытках запугивания сохраняйте доказательства и обращайтесь в правоохранительные органы.

«Ваша карта заблокирована»

В каких случаях такое сообщение может оказаться плохой новостью и при чем тут мошенники

БАНКИ ОБЯЗАНЫ ПРОТИВОДЕЙСТВОВАТЬ ОТМЫВАНИЮ НЕЗАКОННЫХ ДОХОДОВ И МОШЕННИЧЕСТВУ. ПОЭТОМУ ОНИ ОСТАНАВЛИВАЮТ ОПЕРАЦИИ, КОТОРЫЕ СЧИТАЮТ ПОДОЗРИТЕЛЬНЫМИ, И БЛОКИРУЮТ КАРТЫ КЛИЕНТОВ. В НЕКОТОРЫХ СИТУАЦИЯХ БЛОКИРОВКУ МОЖНО СНЯТЬ СРАЗУ, ПОЗВОНИВ В БАНК. НО **ЕСЛИ ОПЕРАЦИЯ ВСЕРЬЕЗ НАСТОРОЖИЛА БАНК, КЛИЕНТУ ПРИДЕТСЯ ДОКАЗЫВАТЬ СВОЮ НЕПРИЧАСТНОСТЬ К ДЕЛАМ МОШЕННИКОВ.** РАЗБИРАЕМСЯ, КАК ВЕСТИ СЕБЯ, ЕСЛИ КАРТА ОКАЗАЛАСЬ ЗАБЛОКИРОВАННОЙ, И МОЖНО ЛИ ЭТО ПРЕДОТВРАТИТЬ.

текст: Юлия СОЛОВЕЙ

Почему банк заблокировал карту

Обнаружил подозрительную операцию

В рамках закона 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» банки должны выявлять подозрительные операции. К ним относится, например, перевод с карты на счет, ранее задействованный в схемах мошенников, внезапное поступление крупной суммы или множества переводов от разных людей.

Если перевод на мошеннический счет произошел с карты впервые, банк остановит его, но может запросить у клиента разъяснения о цели перевода. Если клиент не объяснит или если сумма очень крупная, банк может заблокировать карту и ограничить доступ в мобильное приложение и онлайн-банк. Особенно если перевод с карты по реквизитам из черного списка происходит не впервые. В течение 5 дней после блокировки банк должен уведомить клиента, что послужило ее причиной. Если он этого не сделал, клиенту нужно самостоятельно обратиться в банк с претензией и потребовать назвать причину блокировки карты. Если через 15 рабочих дней банк не ответит, следует писать в интернет-приемную Центрального банка.

Для снятия блокировки с карт и онлайн-банка клиенту нужно будет доказать непричастность к мошенничеству, то есть обосновать происхождение поступившей суммы или разъяснить, почему разные люди переводили ему деньги.

Подозревает мошенническую схему или дроперство

Когда банк видит, что по карте клиента проходит нетипичная операция, он подозревает участие мошенников. Например, человек среди ночи заходит в приложение банка и все деньги переводит на счет, на который никогда раньше ничего не переводил. В этом случае банк на 48 часов замораживает транзакцию, блокирует карту и пытается по телефону или через приложение связаться с клиентом, чтобы получить от него разъяснения об операции. Если за 48 часов клиент не отреагирует на звонки и сообщения банка, блокировка снимется автоматически.

Банк может заподозрить в дроперстве и клиента. Например, если тот стал жертвой схемы «ошибочный перевод». Она работает так: мошенник обманом заставляет жертву перевести деньги на карту, принадлежащую третьему лицу, а затем звонит получателю перевода и просит вернуть, но на другие реквизиты. Так ничего не подозревающий человек случайно попадает как дроп в черный список ЦБ — базу ФинЦЕРТ. Ему ограничивают сумму переводов и снятия наличных в банкомате (не более 100 000 руб. в месяц), а также могут заблокировать карты и доступ в онлайн-банк.

Стопроцентной гарантии, что банк не заблокирует вашу карту, нет. Сегодня банки обязаны проявлять подозрительность в отношении операций по картам клиентов из-за активности мошенников.

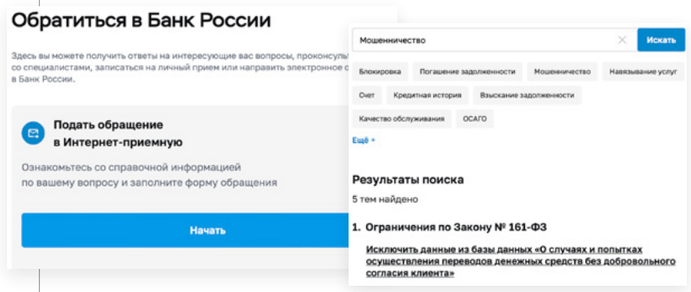
Если вы случайно попали в черный список ЦБ

Так называют базу ФинЦЕРТ, которую ведет спецподразделение Центробанка по кибербезопасности. В нее банки, МВД и другие организации присылают данные о гражданах, по чьим счетам были замечены незаконные операции.

Для исключения своих данных из базы ФинЦЕРТ человеку нужно подать заявление через интернет-приемную на сайте ЦБ или через любой банк, клиентом которого он является. После рассмотрения обращения клиенту должны сообщить идентификатор операции, которая стала причиной его включения в черный список. Затем нужно подать заявление в банк об отказе от зачисления — для этого и нужен идентификатор перевода. В течение 3 дней банк получателя перевода должен вернуть его в банк отправителя.

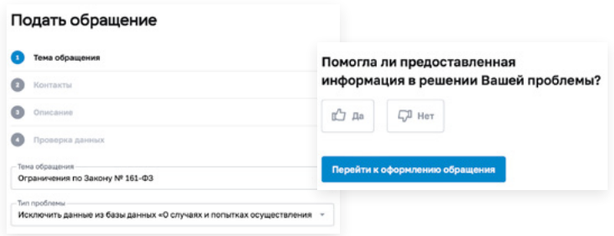
ИНСТРУКЦИЯ

Как подать заявление на исключение из базы ФинЦЕРТ онлайн



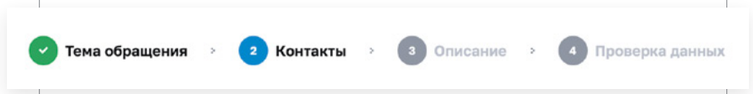
1 На сайте ЦБ РФ **(cbr.ru)** в разделе «Сервисы» выберите «Обратиться в банк России — «Подать обращение в Интернет-приемную» — «Начать» — «Направить обращение»;

2 Под строкой поиска выберите «Мошенничество» — «Исключить данные из базы данных "О случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента"»;



3 Прочитайте справочную информацию на странице: в ней разъясняется порядок процедуры и даже есть примерный шаблон обращения;

4 Нажмите на кнопку «Перейти к оформлению обращения» (она находится ниже справочной информации);



5 Пройдите авторизацию через «Госуслуги», заполните заявление и отправьте его в ЦБ.

После зачисления средств на счет пострадавшего его банк уведомляет ЦБ об отмене операции. На основании этого регулятор будет принимать решение об исключении данных гражданина из базы ФинЦЕРТ. После реабилитации гражданина все блокировки с его счетов снимут и вернут доступ в банковские приложения и онлайн-банк. С учетом 15 рабочих дней, которые даются ЦБ на рассмотрение заявления, реабилитация может оказаться небыстрой.

Если карту заблокировал не банк, а мошенники

Злоумышленник, располагая информацией из утекших баз данных, может от имени жертвы связаться с ее банком и заблокировать карту под предлогом потери. После этого он звонит или пишет жертве, сообщает, что карта заблокирована, и требует деньги за разблокировку. Чтобы напугать и не дать человеку подумать, жулик говорит, что знает данные карт всех родственников и тоже их заблокирует, если не получит деньги. Но тогда, стращает преступник, придется платить уже за разблокировку всех карт.

Если такое произошло, сразу прекратите общение с мошенником, ни в коем случае не делайте то, что он требует. Проверьте статус карты в банковском приложении. Если она на самом деле заблокирована, позвоните в банк и узнайте, по какой причине. Заявите, что вы не давали банку поручения блокировать карту, поясните, при каких обстоятельствах узнали о блокировке. Банк может снять блокировку сразу или попросит прийти в отделение с паспортом.

Как избежать блокировки

Стопроцентной гарантии, что банк не заблокирует вашу карту, нет. Сегодня банки обязаны проявлять подозрительность в отношении операций по картам клиентов из-за активности мошенников. Но если соблюдать правила безопасности, то шансы не столкнуться с блокировкой и не стать жертвой мошенничества выше.

- Не переводите деньги незнакомым людям, чтобы случайно не стать участником мошеннических схем. Если пришлось сделать такой перевод (например, перевели частному мастеру за стрижку деньги на карту, потому что терминал не работал, а наличных с собой не было), укажите в комментарии назначение перевода: оплата за стрижку.
- Если ждете поступления очень крупной суммы на счет или сами будете переводить ее, предупредите об этом заранее свой банк. И будьте готовы подтвердить происхождение денег документами. К примеру, если они от продажи недвижимости или машины, все прояснит для банка договор купли-продажи.
- При продаже вещей на площадках объявлений, принимайте расчет за товар через сервис площадки, а не прямым переводом от покупателя на вашу карту. В противном случае попросите указать назначение перевода — «оплата за велосипед, купленный по объявлению» или что-то в этом роде.
- Ошибочные переводы возвращайте только через процедуру отмены в банке, ни в коем случае не отправляйте деньги сами, особенно если просят вернуть не на тот счет, откуда поступил перевод, а на другой.
- Защитите свои аккаунты надежными паролями, настройте двухфакторную аутентификацию, где это возможно, чтобы мошенники не могли получить доступ к учетным записям и персональным данным. Особенно это касается «Госуслуг», онлайн-банка и банковских приложений.
- Не сообщайте никому данные банковской карты, не называйте коды из СМС — их просят только мошенники, чтобы авторизоваться в чужом аккаунте и получить доступ к деньгам или персональным данным.

ВАЖНО

11 ПРИЗНАКОВ ПОДОЗРИТЕЛЬНОЙ ОПЕРАЦИИ ПО КАРТЕ

1 Реквизиты получателя значатся в базе ФинЦЕРТ и/или в собственном списке подозрительных операций, который ведет банк;

2 Для перевода денег использовалось устройство, применявшееся мошенниками и попавшее в черный список ЦБ;

3 Клиент совершил нетипичный перевод по сумме, времени выполнения или периодичности;

4 В отношении получателя возбуждено уголовное дело о мошенничестве;

5 Наличие данных от других организаций, указывающих на риск мошенничества (например, от сотового оператора о росте числа сообщений или звонков с незнакомых номеров).

6 При бесконтактной операции в банкомате (через карту/смартфон с модулем NFC) время обмена данными между картой (в т. ч. цифровой) и банкоматом превышает норму, установленную Национальной системой платежных карт (НСПК).

7 НСПК проинформировала банк о риске мошенничества при совершении перевода.

8 За 48 часов до перевода произошла смена номера телефона в онлайн-банке или на «Госуслугах»; на устройстве клиента, которое используется для переводов, обнаружены указывающие на риск мошенничества факторы (например, вредоносная программа для считывания логинов и паролей).

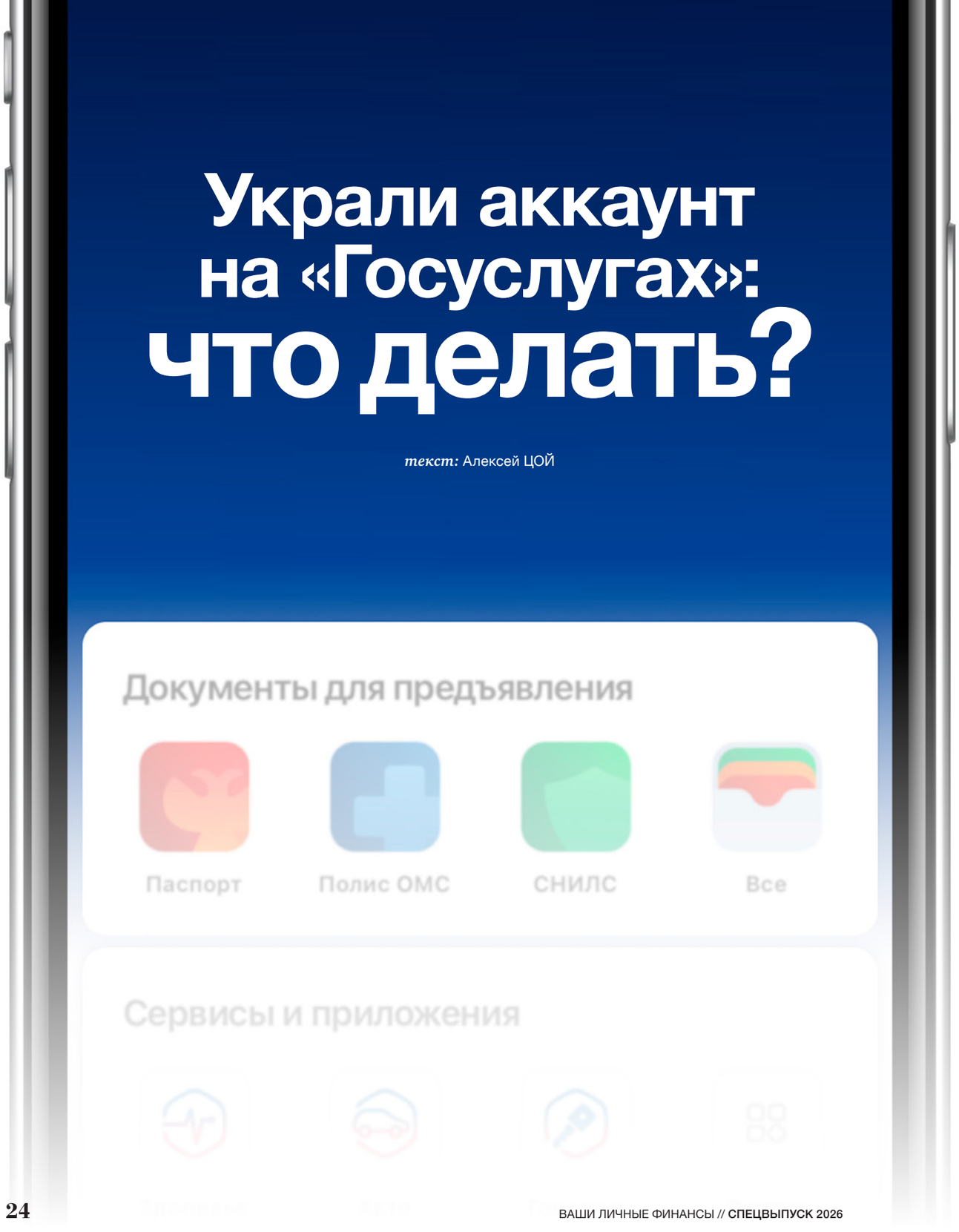
9 Попытка внесения наличных на счет человека с использованием цифровой карты через банкомат, если владелец этого счета за последние 24 часа до этого переводил за границу в адрес физического лица больше 100 000 рублей;

10 Перевод денег человеку, с которым за последние полгода не было финансовых взаимоотношений, при условии, что меньше чем за 24 часа до этого отправитель перевел самому себе из другого банка через СБП больше 200 000 рублей;

11 Сведения о получателе денег содержатся в государственной информационной системе противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий.

Украли аккаунт на «Госуслугах»: что делать?

текст: Алексей ЦОЙ



ПОДТВЕРЖДЕННЫЙ АККАУНТ НА «ГОСУСЛУГАХ» СОДЕРЖИТ ОЧЕНЬ МНОГО ИНФОРМАЦИИ О ЕГО ВЛАДЕЛЬЦЕ — **ДАННЫЕ ПАСПОРТА, ПРОПИСКА, ИМУЩЕСТВО В СОБСТВЕННОСТИ И ТАК ДАЛЕЕ. ВСЕ ЭТО МОГУТ ИСПОЛЬЗОВАТЬ МОШЕННИКИ, ЧТОБЫ НАЖИТЬСЯ ЗА СЧЕТ ЖЕРТВЫ.** ПОЭТОМУ И НЕ ОСТАВЛЯЮТ ПОПЫТОК ПОЛУЧИТЬ ДОСТУП К УЧЕТНЫМ ЗАПИСЯМ РОССИЯН НА ПОРТАЛЕ. КАКИЕ СХЕМЫ ПРИМЕНЯЮТ ЗЛОУМЫШЛЕННИКИ, КАК ЗАЩИТИТЬ СВОЙ АККАУНТ ОТ КРАЖИ И ЧТО ДЕЛАТЬ, ЕСЛИ ЕГО УГНАЛИ?

Кража аккаунта: как происходит и каковы последствия

Для авторизации на «Госуслугах» прежде всего нужны учетные данные — логин и пароль. Мошенники пускают в ход разные средства и методы, чтобы их заполучить: фишинг, социальную инженерию, вредоносные программы. Когда есть логин и пароль, остается последний барьер — код из СМС, который приходит на телефон. Жулик звонит жертве и с помощью какой-то легенды заставляет назвать этот код. После авторизации в аккаунте злоумышленник обычно сразу меняет пароль, чтобы владелец не мог вернуть себе контроль над учетной записью. Чем пользователю угрожает угон аккаунта на «Госуслугах»? Как минимум мошенники могут продать его персональные данные. И если не сами поживятся за счет жертвы, то предоставят эту возможность другим преступникам. Также жулики могут авторизоваться через «Госуслуги» на сайтах микрофинансовых организаций и в личном кабинете налогоплательщика, что позволит им оформить на жертву займы (если не установлен самозапрет) или получить за нее налоговый вычет. Кроме того, информация о человеке дает преступникам исходные данные для разработки персонализированных схем обмана.

Как вернуть доступ к угнанному акканту

Если мошенники не успели поменять пароль, можно по горячим следам успеть «выхватить» у них свой аккаунт. На странице авторизации «Госуслуг» выберите «Восстановить», укажите телефон или электронную почту и нажмите «Продолжить». Затем нужно подтвердить действие: кодом из СМС, если входили по номеру телефона и переходом по ссылке из письма, если логином была почта. Обязательно пробуйте оба способа: если не удалось войти по номеру телефона, попытайтесь через электронную почту. Удалось войти — сразу же поставьте новый пароль.

Проверьте, что в профиле (раздел «Учетная запись») указаны именно ваша почта и телефон. Если нет, то нужно будет поменять их. Это можно сделать онлайн, если вы клиент банка-партнера «Госуслуг», или же лично в МФЦ.

МИНИ-ИНСТРУКЦИЯ

Как восстановить доступ на «Госуслуги», если аккаунт увели мошенники

1. На странице входа выберите «Восстановить» и попробуйте войти по номеру телефона или по электронной почте;

2. Если не получилось, проверьте список банков-партнеров портала: есть ли там ваш банк? Если есть, зайдите в его приложение/личный кабинет на сайте банка и в разделе «Безопасность» пробуйте восстановить доступ к «Госуслугам»;

3. Если предыдущие шаги не помогли, идите с документами (паспорт и СНИЛС) в МФЦ.

Список банков-партнеров для восстановления доступа на «Госуслуги»

Если ни по номеру телефона, ни по адресу электронной почты восстановить доступ в аккаунт не удалось, значит, мошенники сбросили пароль. Тогда можно попробовать вернуть доступ на «Госуслуги» через банк-партнер. Зайдите в приложение или в личный кабинет на сайте банка и найдите раздел «Безопасность» — обычно именно там находится опция восстановления аккаунта на «Госуслугах». Но она сработает, только если мошенники не поменяли либо не установили на портале контрольный вопрос. Если не помогла процедура восстановления через банк, тогда нужно идти с паспортом и СНИЛС в МФЦ.

Как проверить, что делали мошенники через аккаунт

После восстановления доступа к аккаунту нужно проверить, какие действия совершали мошенники. Зайдите в свой профиль, выберите «Безопасность» — «Действия в системе». Отобразятся дата и время авторизации, IP-адрес устройства, с которого мошенник входил в ваш аккаунт, история запросов документов и переходов на другие ресурсы. Над списком действий будет ссылка «Выйти на других устройствах» — нажмите «Выйти», чтобы «выбросить» из аккаунта все устройства, кроме вашего.

А теперь изучите историю действий. Обратите внимание, были ли переходы с портала на другие сайты, обозначенные как «Переход в систему в рамках единой сессии...», — их нужно заскринить и сохранить скриншоты. Если злоумышленник переходил на сайт банка, МФО или налоговой, скорее всего хотел оформить кредит или получить вместо вас вычет. Через пару недель запросите свою кредитную историю и проверьте, нет ли там заявок на кредиты или выданных займов, которые вы не брали.

Проверьте раздел профиля «Сим-карты»: не оформил ли злоумышленник на ваше имя новый номер. Если увидели такой, кликните по нему, выберите в меню «Действия» — «Заблокировать номер». Если есть усиленная квалифицированная электронная подпись (УКЭП), можно сразу выбирать пункт «Расторгнуть договор с оператором связи». Без УКЭП придется идти в офис оператора лично, поскольку блокировка номера — мера временная. Можно сразу заодно поставить самозапрет на оформление новых сим-карт.

Через личный кабинет на сайте ФНС запросите справку об открытых на ваше имя счетах и электронных кошельках: мошенники могли открыть на ваше имя счет, чтобы потом отмывать через него деньги. Так что вы могли стать дропом, сами того не зная.

Что делать, если мошенник оформил на вас кредит

В этом случае придется доказывать, что это были не вы, а именно мошенник, укравший ваш аккаунт на «Госуслугах». Сходите в банк, куда злоумышленник отправил заявку на кредит, и объясните, что ваш аккаунт был украден, попросите аннулировать заявку. Если деньги мошеннику уже выдали, запросите у банка копию заявки на кредит и копию паспорта, по которому его оформили. С документами из банка, а также со скриншотами страницы с историей действий в аккаунте идите в полицию. У вас примут заявление и выдадут талон-уведомление. С этим документом нужно прийти в кредитную организацию, выдавшую заем, и написать заявление о том, что оформлен он не вами, а мошенником, который завладел вашим аккаунтом на «Госуслугах».

ДЕТАЛИ

Период охлаждения по кредитам

Так называется пауза, которую берет банк перед тем, как зачислить кредитные деньги на счет заемщика.

4 часа — 50—200 тысяч ₽

Длительность периода зависит от суммы кредита:

48 часов — больше 200 тысяч ₽

Такая отсрочка защищает заемщика от импульсивных трат: есть время подумать о целесообразности покупки на кредитные деньги, пока они еще не на руках.

Во-вторых, период охлаждения поможет пользователям «Госуслуг», аккаунт которых украли мошенники: если быстро восстановить доступ, можно попробовать отменить займы, оформленные злоумышленниками, пока кредитор еще не выдал им деньги.

Если банк/МФО откажется аннулировать кредит, жалуйтесь в ЦБ (если кредитор —банк) или финансовому омбудсмену (если заем выдан МФО). Если и в этом случае не получится отменить мошеннический кредит, придется доказывать в суде, что вы стали жертвой мошенника.

Если никаких подозрительных действий в аккаунте не обнаружено, кредитная история в порядке, о факте кражи аккаунта все равно нужно сообщить в полицию. В случае использования ваших персональных данных или счетов мошенниками вам будет проще доказать свою непричастность, ведь вы сразу же заявили правоохранителям о взломе.

Спустя полгода повторно запросите кредитную историю и проверьте, что там точно нет кредитов, которые вы не брали. Если с передачей информации от кредитора в БКИ произошла заминка, то данные о мошенническом займе на момент вашего первого запроса там могли еще отсутствовать.

Как защитить аккаунт от мошенников

- Никому и ни под каким предлогом не сообщайте код из СМС от «Госуслуг» — его просят только мошенники.
- Установите контрольный вопрос на портале — без него мошенники не смогут сбросить пароль.
- Придумайте надежный пароль, в котором не менее 10—12 знаков, есть заглавные и строчные буквы, цифры и спецсимволы. Используйте его только на «Госуслугах» и больше нигде.
- Не переходите по ссылкам от неизвестных контактов и не загружайте файлы, чтобы не установить на свое устройство вредоносную программу, передающую мошенникам все логины и пароли.
- Используйте антивирус на всех устройствах.
- Не авторизуйтесь на сайтах и в приложениях, когда используете общественный вайфай. Если нужно где-то авторизоваться, переключитесь на мобильный интернет.
- Если пришло уведомление о входе в учетную запись на «Госуслугах», но вы туда не входили, сбросьте старый пароль и поставьте новый. А также сообщите о попытке угона аккаунта в службу поддержки портала.
- Добавьте доверенный контакт — пользователя «Госуслуг» (это может быть родственник или знакомый, которому доверяете), который будет подтверждать восстановление пароля от вашего аккаунта. Без кода, высылаемого порталом на телефон доверенного контакта, мошенники не смогут сбросить пароль.

ЗАКОН

Новые правила для борьбы с мошенническими займами

Относительно недавно государство ввело меры для противодействия мошенникам, оформляющим кредиты на чужое имя в МФО.

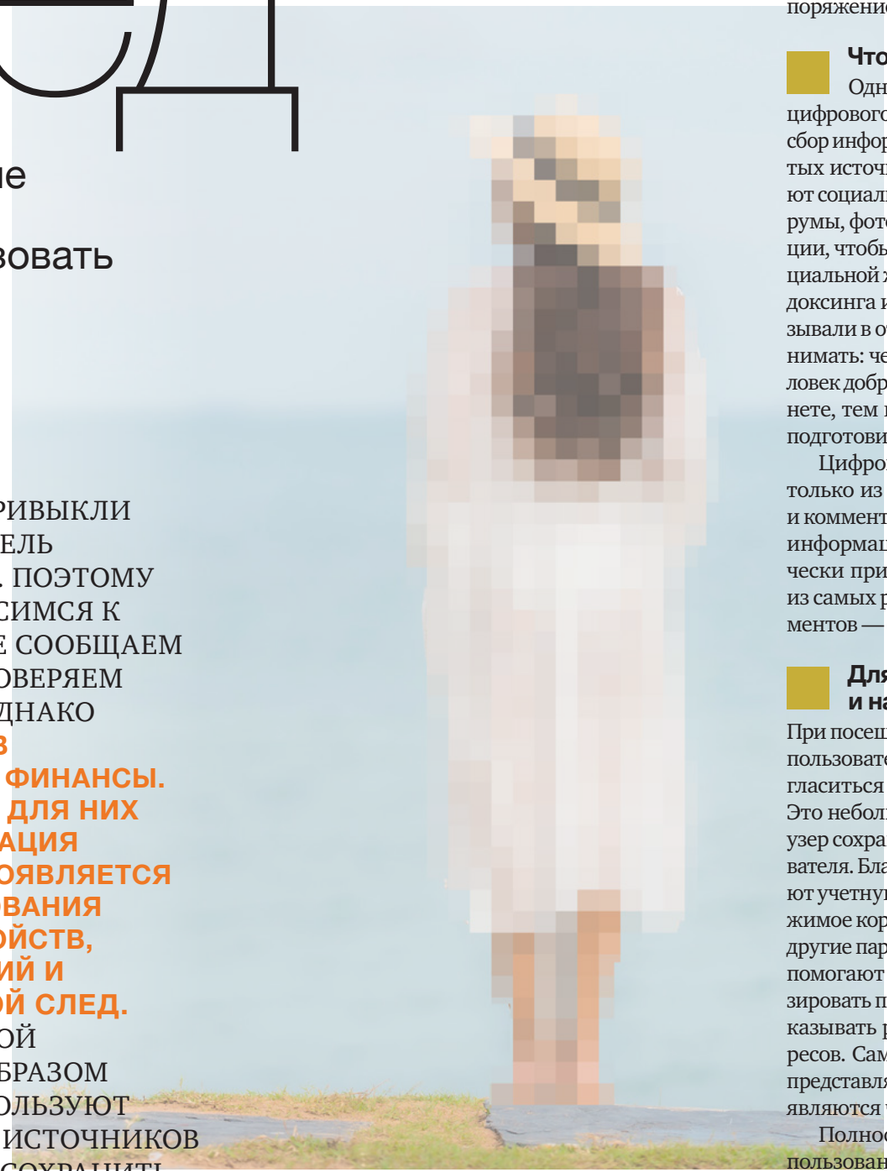
Во-первых, с сентября 2025 года микрофинансовые организации должны перед перечислением денег убедиться, что счет зачисления принадлежит именно тому человеку, который подал заявку на кредит.

А с 1 марта 2026 года идентифицироваться в МФО для оформления займа онлайн можно только по биометрии.

текст:
Юлия ФАЛЛЕР

Цифровой след

Как сохранить личные данные и не дать мошенникам использовать их против вас



БОЛЬШИНСТВО ЛЮДЕЙ ПРИВЫКЛИ СЧИТАТЬ, ЧТО ГЛАВНАЯ ЦЕЛЬ МОШЕННИКОВ — ДЕНЬГИ. ПОЭТОМУ МЫ ВНИМАТЕЛЬНО ОТНОСИМСЯ К БАНКОВСКИМ КАРТАМ, НЕ СООБЩАЕМ НИКОМУ ПИН-КОДЫ И ПРОВЕРЯЕМ ОПЕРАЦИИ ПО СЧЕТАМ. ОДНАКО **СЕГОДНЯ ПРЕСТУПНИКОВ ИНТЕРЕСУЮТ НЕ ТОЛЬКО ФИНАНСЫ. НЕ МЕНЬШУЮ ЦЕННОСТЬ ДЛЯ НИХ ПРЕДСТАВЛЯЕТ ИНФОРМАЦИЯ О ЧЕЛОВЕКЕ, КОТОРАЯ ПОЯВЛЯЕТСЯ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ИМ ЭЛЕКТРОННЫХ УСТРОЙСТВ, МОБИЛЬНЫХ ПРИЛОЖЕНИЙ И ИНТЕРНЕТА, — ЦИФРОВОЙ СЛЕД.** РАЗБЕРЕМСЯ, ЧТО ОН СОБОЙ ПРЕДСТАВЛЯЕТ, КАКИМ ОБРАЗОМ ЗЛОУМЫШЛЕННИКИ ИСПОЛЬЗУЮТ СВЕДЕНИЯ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ И КАКИЕ МЕРЫ ПОМОГУТ СОХРАНИТЬ КОНФИДЕНЦИАЛЬНОСТЬ ЛИЧНОЙ ИНФОРМАЦИИ.

Почему цифровой след требует внимания

Практически ежедневно мы взаимодействуем с цифровыми сервисами. Оплачиваем покупки, вызываем такси, заказываем товары, пользуемся «Госуслугами», ищем информацию, оставляем отзывы и просматриваем сайты. Каждое из этих действий сопровождается сохранением определенных данных.

По отдельности такие сведения редко вызывают опасения. Однако они позволяют составить точное представление о человеке: определить его интересы, привычки, примерный уровень дохода, круг общения и образ жизни. Этой информацией пользуются не только рекламные платформы и интернет-магазины. Она может заинтересовать и мошенников, которым уже не всегда требуется взламывать аккаунты. Зачастую достаточно внимательно изучить открытые страницы пользователя, чтобы подготовить убедительный сценарий обмана.

Что называют цифровым следом

Это совокупность сведений, которые появляются в результате использования интернета, мобильных приложений и электронных устройств. Часть информации пользователь предоставляет самостоятельно: создает учетные записи, размещает публикации, оставляет комментарии, оформляет заказы, заполняет анкеты и делится фотографиями. Другая часть формируется автоматически за счет фиксации интернет-ресурсами технических характеристик устройства, истории посещений, продолжительности пребывания на страницах, поисковых запросов, интереса к определенным товарам и примерного местоположения.

Даже если отдельные данные кажутся незначительными, вместе они способны рассказать о человеке гораздо больше, чем может показаться на первый взгляд. Поэтому специалисты по информационной безопасности рекомендуют относиться к персональным данным так же внимательно, как к документам или банковским картам. Сам по себе цифровой след нельзя назвать угрозой. Он становится опасным тогда, когда накопленные сведения попадают в распоряжение злоумышленников.

Что такое доксинг

Одной из главных опасностей цифрового следа является доксинг — сбор информации о человеке из открытых источников. Мошенники изучают социальные сети, объявления, форумы, фотографии и другие публикации, чтобы собрать сведения о потенциальной жертве. Подробнее о работе доксинга и его опасности мы рассказывали в отдельной статье. Важно понимать: чем больше информации человек добровольно оставляет в интернете, тем проще злоумышленникам подготовить мошенническую схему.

Цифровой след складывается не только из фотографий, публикаций и комментариев. Значительная часть информации собирается автоматически при посещении сайтов. Один из самых распространенных инструментов — файлы Cookie.

Для чего нужны Cookie и надо ли их удалять

При посещении большинства сайтов пользователи видят предложение согласиться на использование Cookie. Это небольшие файлы, которые браузер сохраняет на устройстве пользователя. Благодаря им сайты запоминают учетную запись, настройки, содержимое корзины интернет-магазина и другие параметры. Кроме того, Cookie помогают владельцам сайтов анализировать поведение посетителей и показывать рекламу с учетом их интересов. Сами по себе такие файлы не представляют опасности, однако тоже являются частью цифрового следа.

Полностью отказываться от использования файлов Cookie обычно нет необходимости, поскольку многие интернет-ресурсы без них работают менее удобно. Но периодическая их очистка будет полезна, особенно если вы пользовались чужими устройствами совместно с другими людьми или хотите сократить объем накопленной информации о своей активности. Во многих современных браузерах также можно отключить сторонние Cookie, которые чаще всего используются рекламными сетями для отслеживания поведения пользователей.

Какие сведения лучше не публиковать

Вот что эксперты по цифровой безопасности советуют не размещать в открытом доступе:

- фотографии документов;
- изображения банковских карт;
- посадочные талоны;
- чеки с QR-кодами;
- домашний адрес;
- государственные регистрационные номера автомобилей;
- документы с личными данными.

Желательно не сообщать о поездках и длительном отсутствии дома в режиме реального времени.

Что важно помнить о мессенджерах и социальных сетях

Многие считают, что сообщения в мессенджерах или комментарии в социальных сетях исчезают бесследно после удаления. На практике это не всегда так. Сообщение могли успеть прочитать другие пользователи, сделать снимок экрана, переслать его знакомым или сохранить с помощью специальных сервисов.

В некоторых случаях копии информации могут оставаться на серверах сервисов или в поисковых системах еще некоторое время. Поэтому любое сообщение, фотографию или комментарий стоит публиковать так, словно они могут сохраниться надолго. Если запись уже появилась в интернете, нельзя рассчитывать, что после удаления о ней никто не узнает.

Инструменты для защиты конфиденциальности

Дополнительную защиту дают современные средства обеспечения циф-

ровой безопасности. Браузеры с расширенными настройками приватности ограничивают сбор пользовательских данных и блокируют работу рекламных трекеров. Полезными могут оказаться специальные расширения, автоматически удаляющие Cookie, препятствующие отслеживанию действий пользователя и уменьшающие количество навязчивой рекламы. Однако даже самые современные технологии не заменяют внимательности самого пользователя.

Смартфон — источник большого объема личной информации

Современный смартфон хранит огромное количество конфиденциальных данных: банковские приложения, фотографии, переписку, контакты, документы, историю перемещений и другую личную информацию. Именно поэтому важно периодически проверять разрешения, которые получают установленные приложения. Не менее важно своевременно обновлять операционную систему, удалять ненужные приложения, использовать блокировку экрана и биометрические способы защиты устройства.

Как удалить информацию о себе из интернета и соцсетей

Полностью стереть цифровой след не получится: информация, однажды попавшая в интернет, может еще долго храниться в поисковых системах, архивах сайтов или базах данных различных сервисов. Но сократить количество личной информации в открытом доступе вполне реально. Начните со старых аккаунтов. Возможно, у вас до сих пор есть страницы на форумах, в интернет-магазинах, сервисах бронирования или социальных сетях, которыми вы давно не пользуетесь. Часто такие профили содержат номер телефона, адрес электронной почты, фотографии и другую личную информацию. Если аккаунт больше не нужен, лучше удалить его полностью.

Затем стоит посмотреть на свои страницы в социальных сетях. Старые фотографии, публикации из путешествий, отметки с геолокацией, информация о месте работы или учебы, снимки документов и даже обычные комментарии могут рассказать о вас гораздо больше, чем кажется. Если какие-то публикации уже потеряли актуальность или содержат слишком много личных сведений, их лучше удалить или скрыть.

Загляните в настройки конфиденциальности. Многие соцсети позволяют выбрать, кто может видеть ваши фотографии, список друзей, номер телефона, дату рождения и другие данные. Несколько минут, потраченных на эти настройки, помогут значительно сократить объем информации, доступной незнакомым людям.

Еще одна полезная привычка — время от времени искать себя в интернете. Введите в поисковой системе свое имя, адрес электронной почты или номер телефона и посмотрите, какая информация доступна любому пользователю. Если найдете устаревшие или нежелательные сведения, можно обратиться к владельцу сайта с просьбой удалить их. После этого поисковые системы постепенно перестанут показывать удаленные страницы.

Если ваши данные уже используют мошенники

Если злоумышленники уже связались с вами, важно сохранять спокойствие и не действовать поспешно. Специалисты рекомендуют:

- не вступать в переписку с мошенниками;
- не выполнять их требования;
- изменить пароли электронной почты, соцсетей и банковских сервисов;
- включить двухфакторную аутентификацию, если она не используется;
- сохранить сообщения, номера телефонов и другие возможные доказательства;
- предупредить родственников о вероятных мошеннических звонках;
- при необходимости обратиться в банк и правоохранительные органы.

текст:
Юлия ФАЛЛЕР

Инструменты безопасности в MAX: как защитить аккаунт от мошенников и нежелательных контактов

НАЦИОНАЛЬНЫЙ МЕССЕНДЖЕР MAX ПРЕДЛАГАЕТ **РАЗНЫЕ МЕХАНИЗМЫ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ БЕЗОПАСНОСТИ АККАУНТА. ЧАСТЬ ИЗ НИХ ОРИЕНТИРОВАНА НА ЗАЩИТУ САМОГО ПОЛЬЗОВАТЕЛЯ, А ДРУГАЯ — НА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЧЛЕНОВ СЕМЬИ.** ИСПОЛЬЗОВАНИЕ ЭТИХ ФУНКЦИЙ ПОМОГАЕТ СНИЗИТЬ ВЕРОЯТНОСТЬ ОБЩЕНИЯ С МОШЕННИКАМИ, ОГРАНИЧИТЬ НЕЖЕЛАТЕЛЬНЫЕ КОНТАКТЫ И СОХРАНИТЬ КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ.

«Семейная защита» — контроль настроек без доступа к переписке

Одним из наиболее востребованных инструментов стала функция «Семейная защита», позволяющая назначить администратора безопасности для аккаунта ребенка, пожилого родственника или другого близкого человека.

Главное преимущество функции в том, что она не нарушает личное пространство пользователя. Администратор безопасности не получает доступа к сообщениям, фотографиям, истории звонков или контактам. Он лишь управляет настройками приватности, которые позволяют ограничить взаимодействие с незнакомыми людьми и потенциально опасными аккаунтами.

После подключения функции можно дистанционно изменить несколько важных параметров безопасности:

- разрешить входящие звонки только от пользователей из телефонной книги;
- запретить личные сообщения от незнакомых людей;
- ограничить возможность добавления пользователя в групповые чаты;
- включить фильтрацию контента с возрастными ограничениями 16+ и 18+.

Кроме того, если система выявит подозрительную активность — например, попытку добавить защищаемого пользователя в сомнительную группу или контакт, который алгоритмы распознают как потенциально опасный, — администратор безопасности получит уведомление и сможет своевременно принять меры. Такой подход особенно полезен для семей с детьми, а также для пользователей старшего поколения, которые не всегда знакомы с современными схемами интернет-мошенничества и могут доверять сообщениям, поступающим от незнакомых людей.

Как подключить «Семейную защиту»

Перед началом настройки рекомендуется убедиться, что на обоих устройствах установлена последняя версия приложения MAX. Новые функции безопасности становятся доступны только после обновления. Подключение занимает всего несколько минут.

- Шаг 1. Убедитесь, что пользователи добавлены друг у друга в контактах.
- Шаг 2. На устройстве администратора откройте раздел «Настройки» «Безопасность» (или «Приватность») «Семейная защита» и выберите пункт «Создать защиту».
- Шаг 3. Полученный шестизначный код необходимо передать защищаемому пользователю. Код действует только десять минут и используется один раз.
- Шаг 4. На втором устройстве откройте раздел «Семейная защита», выберите пункт «Вступить по коду» и введите полученный код.
- Шаг 5. После завершения подключения можно выбрать необходимые параметры безопасности исходя из возраста пользователя и его потребностей.

При необходимости функцию можно отключить в любой момент, удалив пользователя из списка «Семейной защиты». После этого удаленное управление настройками прекращается.

Безопасный режим

Режим предназначен для быстрого повышения уровня конфиденциальности и активируется одним переключателем. После включения автоматически применяются сразу несколько параметров безопасности:

- профиль скрывается из поиска;
- звонки принимаются только от сохраненных контактов;
- приглашения в групповые чаты разрешаются только знакомым пользователям;
- включается фильтр контента категории 18+.

Это удобное решение для тех, кто не хочет вручную изменять каждую настройку отдельно. Вместе с тем следует помнить, что безопасный режим управляется самим владельцем аккаунта и при необходимости может быть отключен.

Двухфакторная аутентификация

Она остается одной из самых эффективных мер защиты учетной записи. После ее активации для входа в аккаунт потребуется не только код подтверждения из СМС, но и дополнительный облачный пароль, известный только владельцу аккаунта. Даже если злоумышленникам удастся получить доступ к номеру телефона или одноразовому коду, этого будет недостаточно для входа.

Настроить двухфакторную аутентификацию можно в разделе «Приватность». Специалисты по информационной безопасности рекомендуют использовать уникальный сложный пароль, не совпадающий с паролями от других сервисов.

Комплексный подход к безопасности

Наиболее высокий уровень защиты достигается при использовании сразу нескольких механизмов безопасности. Для детей и пожилых родственников целесообразно подключить «Семейную защиту», чтобы ограничить общение с незнакомцами. Для собственного аккаунта рекомендуется активировать безопасный режим и обязательно включить двухфакторную аутентификацию.

ШКОЛЬНИКИ ЕЖЕДНЕВНО ОБЩАЮТСЯ В МЕССЕНДЖЕРАХ, СОЦИАЛЬНЫХ СЕТЯХ И ОНЛАЙН-ИГРАХ, ГДЕ МОГУТ СТОЛКНУТЬСЯ С МОШЕННИКАМИ. **ЗЛОУМЫШЛЕННИКИ ХОРОШО ПОНИМАЮТ ОСОБЕННОСТИ ПОВЕДЕНИЯ ПОДРОСТКОВ И УМЕЮТ ВЫЗЫВАТЬ ДОВЕРИЕ.** ЧЕРЕЗ ПСИХОЛОГИЧЕСКОЕ ДАВЛЕНИЕ И СОЦИАЛЬНУЮ ИНЖЕНЕРИЮ ОНИ ЗАСТАВЛЯЮТ ЖЕРТВУ ПРИНИМАТЬ НЕОБДУМАННЫЕ РЕШЕНИЯ, ЧТОБЫ ПОЛУЧИТЬ ДОСТУП К АККАУНТАМ, ПЕРСОНАЛЬНЫМ ДАННЫМ И ДЕНЬГАМ РОДИТЕЛЕЙ.

текст:
Юлия ФАЛЛЕР

Дети в интер--нете

Как защитить ребенка от мошенников

Как мошенники вовлекают детей в преступные схемы

Одна из наиболее распространенных угроз — телефонное мошенничество через мессенджеры. Преступники все чаще используют их вместо привычных звонков с неизвестных номеров. Во время разговора злоумышленник может представиться сотрудником банка, правоохранительных органов, государственного учреждения, оператора связи или службы безопасности различных сервисов или сотрудником из школы. Чтобы сделать легенду более убедительной, мошенники используют видеозвонки, демонстрируют поддельные удостоверения, логотипы организаций и фальшивые документы. Основная цель подобных действий — убедить ребенка самостоятельно предоставить конфиденциальную информацию или выполнить определенные действия. Например, назвать коды подтверждения из СМС, сообщить пароль, установить программу удаленного доступа, передать данные банковской карты родителей или войти в личный кабинет под диктовку собеседника.

Практически всегда мошенники оказывают сильное психологическое давление. Они торопят, утверждают, что ситуация требует немедленного решения, запугивают возможной блокировкой аккаунта, уголовной ответственностью, потерей денег или проблемами у родителей. В условиях стресса подростку значительно сложнее критически оценить происходящее, поэтому вероятность успешной атаки возрастает.

Еще один распространенный сценарий — вовлечение детей через игровые платформы и социальные сети. Под предлогом получения бесплатной игровой валюты, редких предметов, подарков или участия в розыгрыше злоумышленники просят перейти по ссылке, авторизоваться на поддельном сайте или сообщить данные учетной записи. В результате ребенок может потерять доступ к своему аккаунту, а преступники получат возможность использовать его для дальнейших мошеннических действий.

Помимо кражи персональных данных и денег, мошенники все чаще используют схему «легкий заработок». Несовершеннолетним обещают быстрый доход без опыта и специальных навыков: достаточно выполнить «простое поручение» или предоставить доступ к своему банковскому счету. Чаще всего объявления о подобной работе распространяются через социальные сети, мессенджеры и игровые сообщества. Однако за безобидными предложениями могут скрываться преступные схемы. Подростков просят оформить банковскую карту и передать ее третьим лицам, предоставить реквизиты счета для перевода денег, зарегистрировать аккаунты на свое имя, получить и переслать посылку, снять наличные в банкомате или перевести средства на указанные счета. Нередко такие действия преподносятся как работа курьером, финансовым помощником или посредником.

Фактически несовершеннолетний становится участником схем по обналичиванию и выводу похищенных денежных средств — дропом, одним из многих посредников, через счета которых проходят деньги, полученные преступным путем. Даже если подросток не осознавал противоправный характер своих действий, это не освобождает от возможных правовых последствий. В зависимости от обстоятельств он может стать фигурантом уголовного расследования, а его родители — столкнуться с необходимостью возмещать ущерб.

Если дети уверены, что их не будут ругать за ошибку, они гораздо быстрее рассказывают о подозрительных сообщениях, звонках или попытках выманить личную информацию.

Особо опасны предложения выполнить «разовое задание» за крупное вознаграждение. За этим могут скрываться не только финансовые преступления, но и попытки вовлечения несовершеннолетних в распространение запрещенных веществ, поджоги объектов инфраструктуры, диверсии, мошеннические обзвоны и другие противоправные действия. Организаторы этих схем сознательно используют доверчивость подростков, обещая легкий заработок и уверяя, что никакой ответственности не будет.

Что должно насторожить родителей

Не всегда ребенок сразу рассказывает о попытке обмана. Иногда он испытывает страх, чувство вины или опасается наказания. Поэтому родителям важно обращать внимание не только на технические признаки, но и на изменения в поведении. Поводом для разговора с ребенком могут стать:

- продолжительное общение по телефону или переписка с незнакомыми;
- внезапная тревожность или нервозность после использования телефона;
- повышенная скрытность и нежелание показывать экран устройства;
- появление новых подозрительных контактов в социальных сетях или мессенджерах;
- просьбы срочно воспользоваться банковской картой родителей или их телефоном;
- отказ обсуждать происходящее и резкие изменения привычного поведения ребенка.

Подобные признаки не всегда свидетельствуют о мошенничестве, однако требуют внимания и доверительного общения взрослых с детьми.

Как снизить риск стать жертвой мошенников

Регулярно обсуждайте правила цифровой безопасности

Один разговор не сформирует устойчивые навыки безопасного поведения. Информационная безопасность — это привычка, которая развивается постепенно. Полезно регулярно обсуждать реальные примеры мошеннических схем, объяснять, почему преступники используют давление и манипуляции, вместе анализировать новости о киберпреступлениях. Чем лучше ребенок понимает принципы работы мошенников, тем выше вероятность, что он вовремя распознает опасность. Важно донести простую мысль: если кто-то требует срочно принять решение, сохранить разговор в тайне или выполнить финансовые действия без участия взрослых, это серьезный повод прекратить общение.

Развивайте финансовую грамотность

Финансовая грамотность — важная часть цифровой безопасности. Ребенок должен понимать ценность денег, знать, как работают банковские карты, электронные платежи и системы подтверждения операций. Полезно объяснить, что одноразовые коды, пароли, реквизиты банковских карт и персональные данные никогда нельзя передавать посторонним, даже если они представляются сотрудниками банка или государственных органов.

Карманные деньги, совместное планирование расходов и обсуждение семейного бюджета помогают сформировать ответственное отношение к финансам и снижают вероятность совершения необдуманных действий под влиянием мошенников.

→ С. 34

← С. 33

Используйте возможности банковских сервисов

Если подросток уже пользуется собственной картой, родителям стоит обратить внимание на инструменты, которые предлагают современные банки. Они позволяют отслеживать операции по карте, получать уведомления о расходах, устанавливать лимиты на покупки и переводы, а также при необходимости быстро заблокировать карту. Такие функции помогают не только контролировать финансовую активность ребенка, но и своевременно выявлять подозрительные операции.

Если подросток под влиянием мошенников попытается перевести деньги, предоставить доступ к своему счету или использовать карту для чужих денежных переводов, родители смогут оперативно вмешаться и предотвратить возможные последствия. Это снижает риск необдуманных поступков и помогает защитить ребенка от вовлечения в мошеннические схемы, в том числе связанные с дроперством.

Подключите инструменты родительского контроля

Современные цифровые сервисы позволяют существенно повысить уровень безопасности детей в интернете. Родительский контроль помогает ограничивать установку неизвестных приложений, фильтровать нежелательный контент, контролировать экранное время и получать уведомления о потенциально опасной активности. Важно помнить: технические средства не заменяют доверительного общения. Они должны служить дополнительным инструментом защиты, а не способом тотального контроля.

Создавайте атмосферу доверия

Главная задача родителей — сделать так, чтобы ребенок не боялся обращаться к ним за помощью. Если дети уверены, что их не будут ругать за ошибку, они гораздо быстрее рассказывают о подозрительных сообщениях, звонках или попытках выманить личную информацию. Это позволяет своевременно сменить пароли, заблокировать доступ злоумышленникам и предотвратить финансовые потери. Важно объяснить ребенку, что стать объектом внимания мошенников может любой человек независимо от возраста. Главное — сразу сообщить о проблеме взрослым, а не скрывать ее.

«Вторая рука»

Сервис для защиты денег от мошенников

МОШЕННИКАМ ДО СИХ ПОР УДАЕТСЯ ОБМАНЫВАТЬ РОССИЯН, ВЫНУЖДАЯ ИХ ПЕРЕВОДИТЬ ДЕНЬГИ НА «БЕЗОПАСНЫЙ» СЧЕТ. И ЧАЩЕ ВСЕГО ЭТА СХЕМА СРАБАТЫВАЕТ НА ПОЖИЛЫХ. ДЛЯ ЗАЩИТЫ ДЕНЕГ КЛИЕНТОВ В СЕНТЯБРЕ 2025 ГОДА БАНКИ ЗАПУСТИЛИ СЕРВИС «ВТОРОЙ РУКИ»: **ДАЖЕ ЕСЛИ ЖУЛИКИ УБЕДЯТ ЧЕЛОВЕКА ПЕРЕВЕСТИ ИМ ДЕНЬГИ, СРЕДСТВА НЕ СМОГУТ УЙТИ СО СЧЕТА БЕЗ ОДОБРЕНИЯ ДОВЕРЕННОГО ЛИЦА.** РАССКАЗЫВАЕМ, КАК ЭТО РАБОТАЕТ И КОМУ БУДЕТ ПОЛЕЗНО.

текст: Алексей ЦОЙ

Как работает сервис

Суть работы этого банковского сервиса в назначении доверенного человека, который будет отслеживать определенные виды операций и сможет их отклонять. Ни счета, ни количество денег на них помощник не видит и не может распоряжаться средствами, может только заблокировать операцию или одобрить.

Виды подконтрольных транзакций для «второй руки» выбирает клиент банка — переводы по номеру телефона, реквизитам карты или счета, по QR-коду, снятие наличных через банкомат или оператора в банке, закрытие вклада. Для каждого вида можно установить лимит суммы: если перевод укладывается в него, банк его выполняет, если превышает — запрашивается одобрение доверенного лица. Лимиты нужны, чтобы вашей «второй руке» не приходили на одобрение транзакции вроде оплаты покупок в супермаркете. При этом можно настроить отдельно лимиты для карты, накопительного счета и вклада.

Как это будет работать? Например, банк зафиксировал подозрительную операцию по счету клиента, подключившего сервис «второй руки», — вывод денег со вклада на чужую карту. Банк останавливает транзакцию и отправляет уведомление (пуш или СМС) помощнику клиента. Теперь он должен одобрить или отклонить операцию. Если никакой реакции от «второй руки» нет, банк все равно отменит перевод. Таким образом, если мошенники обманом вынудят пожилого человека перевести им сбережения или сами попытаются вывести их, получив доступ в онлайн-банк жертвы, сервис в любом случае сохранит деньги клиента. А у помощника будет время поговорить с родственником и выяснить все обстоятельства: кому и для чего тот хотел отправить деньги. И даже если по каким-то причинам «вторая рука» не сможет среагировать на запрос банка, деньги не уйдут на счет мошенников.

Стать «второй рукой» полезно и родителям: уведомления от банка о переводах с карты ребенка на карты незнакомцев позволят предотвратить вовлечение детей в дроперство.

Кто может стать «второй рукой» и как подключить сервис

Доверенным помощником может стать любой, кому доверяет клиент банка, необязательно родственник. Но лучше предварительно ввести в курс дела того, кого вы выбрали в качестве «второй руки». И заранее узнать в банке, должен ли потенциальный помощник тоже быть его клиентом, есть ли комиссия за использование сервиса и как происходит смена «второй руки». Между банком, клиентом и «второй рукой» подписывается трехстороннее соглашение, на следующий день сервис начинает работать.

Порядок подключения сервиса определяют сами банки. Где-то требуется прийти вдвоем с помощником в офис банка и написать заявление, в некоторых банках все можно сделать через приложение или личный кабинет на сайте. После заключения соглашения нужно будет настроить параметры работы сервиса — выбрать виды операций для проверки и лимиты сумм для каждой из них. По желанию клиент может сократить время, отведенное на реакцию помощника (по умолчанию это 12 часов).

Если в процессе использования сервиса возникнет необходимость изменить настройки, сделать это можно в любое время, как и отключить сервис. Но следует иметь в виду, что при отключении сервиса и смене доверенного помощника действует 24-часовой период охлаждения. Это сделано опять-таки из-за мошенников: если они обманом убедят человека отключить сервис «второй руки», он не сможет сделать это мгновенно, а значит, появится время подумать, рассказать о ситуации родным и в итоге спасти деньги.

Плюсы и минусы

«Вторая рука» поможет защитить деньги не только от жуликов. Так, людям, склонным к совершению покупок на эмоциях, полезно иметь некий барьер, чтобы не спустить на маркетплейсе ползарплаты из-за плохого настроения и желания себя «порадовать». А еще можно с помощью сервиса уберечь свою финансовую подушку безопасности от собственных посягательств, когда возникает соблазн потратить на что-то, без чего можно обойтись.

К минусам сервиса можно отнести технический фактор: из-за сбоя помощник может не получить уведомление о какой-то важной для его доверителя операции, и банк отменит ее по истечении 12 часов (или раньше, если клиент это настроил).

Региональный центр финансовой грамотности: бесплатные юридические консультации по финансовым вопросам

- Задолженность, высокая долговая нагрузка
- Финансовое планирование
- Наследство
- Банкротство физлиц
- Накопления и сбережения
- Финансовое мошенничество
- Кредитование
- Налоги и пенсионное обеспечение

Как получить консультацию

8-800-201-67-70
По телефону горячей линии

Томск, ул. Гоголя, 15, оф. 401
Записаться и прийти на прием лично в РЦФГ

ВКонтакте | Телеграм | Макс | Сайт

РЦФГ региональный центр финансовой грамотности