Финцентр РБ
грамотные финансовые решения

9 способов
защититься от финансовых мошенников

Чек-лист для защиты от мошенников

Чтобы не перевести деньги мошенникам

• Договоритесь с родными, что переводы денег и оплату услуг в ситуации, когда сумма превышает определенную величину, вы делаете только посоветовавшись с близкими!

Чтобы не допустить утечки данных банковской карты

• Используйте отдельную банковскую карту для оплаты в Интернете и переводите на нее нужную сумму непосредственно перед покупкой

• Регулярно проверяйте выписки по счетам

• Не вводите данные карты на малознакомых сайтах

• Не позволяйте сайтам, браузеру и операционной системе запоминать данные ваших карт

Чтобы не попасться на фальшивые инвестиции

• Не инвестируйте деньги в интернете по объявлениям незнакомцев, кем бы они ни представлялись!

• Проверьте компанию или инвестора в реестре Банка России на сайте cbr.ru в разделе **«Проверить участника финансового рынка»** или по горячей линии (8-800-300-3000, моб. 300)

• Деньги для инвестиций не переводят на счет «агента», «брокера», «наставника» или «куратора» — физического лица

• Вкладывайте в инвестиции только те деньги, которые готовы потерять. Брать кредиты и пускать их в инвестиции — очень плохая затея

• Не ведитесь на то, что смогли вывести первую прибыль. Мошенник даст вам «отбить» первые вложения, чтобы убедить, что схема работает. Ловушка захлопнется не сразу, а когда вы вложите большие суммы

• Запомните: доход в инвестициях не может быть гарантирован!

Чтобы не получать телефонные звонки от мошенников

• Подключите услугу блокировки спама, тогда все подозрительные номера будут отклоняться или сопровождаться уведомлением «возможно, спам». Услуга есть у большинства мобильных операторов, соцсетей, банков и справочных сервисов

• Договоритесь с близкими о кодовом слове для экстренных ситуаций, чтобы отличить их от мошенников во время звонка

Чтобы случайно не загрузить шпионскую программу или вирус

• Не переходите ни по каким ссылкам, не устанавливайте программы, которые вам кто-то прислал. Например, под предлогом обучения при трудоустройстве или установки личного кабинета в инвестициях. Мошенники могут просить скачать на телефон новую версию Госуслуг или усиленный антивирус. На самом деле это программы удаленного доступа, которые показывают все, что происходит на телефоне: от СМС до паролей

• Обновляйте антивирусы на устройствах

Чтобы не попасть на поддельный сайт

• Проверяйте адресную строку сайта, на который переходите. Мошенники часто используют похожие адреса, изменяя одну букву или заменяя ее цифрой

• Официальные сайты банков и микрофинансовых, страховых организаций в поисковой выдаче «Яндекса» и Mail.ru маркируются специальным знаком (синий кружок с галочкой)

Чтобы на вас не оформили кредит или не перевели деньги без вашего ведома

• Установите самозапрет на выдачу кредитов через портал Госуслуг (с 1 сентября 2025 г. самозапрет можно также установить через МФЦ)

• Самозапрет распространяется на НОВЫЕ потребительские кредиты, микрозаймы, кредитные карты. Действующие обязательства останутся неизменными. Самозапрет не действует в случаях, когда человек соберется оформить ипотеку, автокредит, образовательный кредит, т.е. когда деньги не перечисляются заемщику напрямую и риск мошенничества минимален

Чек-лист для защиты от мошенников

Чтобы защитить свои Госуслуги

На сайте Госуслуг есть инструкция «Если учетную запись взломали»

Установите следующие настройки в разделе «профиль» / «безопасность»:

1. Подключите уведомления о входе на Госуслуги — они будут приходить на электронную почту, указанную в личном кабинете
2. Добавьте контрольный вопрос — его будут запрашивать при восстановлении доступа

• **Запомните:** ни одному ведомству не нужен смс-код от Госуслуг. Не сообщайте его никому. Также помните — специалисты Госуслуг не звонят вам и не помогают восстановить доступ. Это делают мошенники!

• Если случайно назвали данные мошенникам, постарайтесь войти в личный кабинет. **Проверьте** раздел «документы» – мошенники могут подгрузить туда фальшивую доверенность и пугать вас этим. Эта доверенность не действительна! Проверьте, ваш ли номер телефона и почта указаны в личном кабинете. **Смените пароль!**

• Если аккаунт Госуслуг взломали, **срочно восстановите** его через офисы МФЦ или другие центры обслуживания. Адреса можно уточнить на сайте Госуслуг. Возьмите с собой паспорт и СНИЛС

• **Напишите заявление** в полицию. Если в будущем мошенники воспользуются вашими данными и оформят кредиты, у вас должно быть доказательство взлома

Чтобы не взломали ваш мессенджер

• Установите двухшаговую проверку на все мессенджеры

• Регулярно проверяйте связанные устройства в настройках мессенджера — это поможет выявить лишнее устройство, которое имеет доступ к вашей переписке

• Не переходите по ссылкам, не загружайте файлы, которые содержатся в сообщениях, даже если они от знакомых

МЫ В СОЦСЕТЯХ
«Деньги к деньгам»
@money02money