# Инструкция

# Как защитить себя от мошенников

## 1. Изучите основные схемы обмана

Знание типичных мошеннических схем — первый шаг к защите. Распространённые варианты:

- **Фишинговые письма и SMS.** Сообщения с ссылками на поддельные сайты банков, «Госуслуг» и т. д. Цель — получить ваши логины, пароли, данные карт.
- **Звонки от «сотрудников банка».** Мошенники представляются работниками службы безопасности банка, сообщают о подозрительной операции и просят назвать реквизиты карты или код из SMS.
- **«Вы выиграли приз».** Вам сообщают о выигрыше (путёвки, техники и т. п.), но для его получения нужно оплатить «налог», «доставку» или ввести данные карты.
- **Инвестиционные ловушки.** Обещают высокую доходность при минимальных вложениях, убеждают перевести деньги на «специальный счёт». Часто используют фейковые отзывы и поддельные графики роста.
- **Мошенничество с арендой жилья.** Показываются объявления с привлекательными условиями, просят внести предоплату или полную оплату, после чего исчезают.
- **Поддельные интернет-магазины.** Сайты с нереально низкими ценами, но после оплаты товар не приходит или приходит подделка.
- **Социальные инженерия и дипфейки.** Использование фото, аудио или видео с помощью ИИ от лица знакомых или авторитетных лиц, чтобы выманить деньги или конфиденциальную информацию.
- **Дропперство.** Предложение «лёгкого заработка»: оформить карту, принимать и пересылать деньги. За участие в таких схемах предусмотрена уголовная ответственность.

## 2. Научитесь распознавать мошенников

Признаки мошеннических действий:

- **Давление и спешка.** Фразы «нужно сделать прямо сейчас», «предложение действует только сегодня», «иначе счёт заблокируют».
- **Апелляция к авторитету.** Представляются сотрудниками банка, полиции, налоговой, прокуратуры и т. д.
- **Вызывают сильные эмоции.** Пугают потерей денег, блокировкой счёта, уголовной ответственностью или, наоборот, соблазняют большой прибылью.
- **Просят конфиденциальную информацию.** Настоящие сотрудники банков и госорганов никогда не спрашивают CVV-код, пароли от аккаунтов, коды из SMS.

- **Ошибки в оформлении.** В письмах и на сайтах могут быть опечатки, неграмотные формулировки, логотипы плохого качества.
- **Необычные способы оплаты.** Просят перевести деньги на карту физлица, электронный кошелёк, криптовалюту вместо официального счёта компании.

Дополнительные советы:

- Не делитесь личной информацией (паспортные данные, СНИЛС, ИНН, коды доступа) ни по телефону, ни в переписке.
- Перед переводом денег или предоставлением данных всегда проверяйте информацию — звоните в организацию по официальному номеру, ищите отзывы.
- Используйте двухфакторную аутентификацию везде, где это возможно.
- Установите антивирус на все устройства и регулярно обновляйте его.

## 3. Настройте безопасность устройств и сервисов

- **Обновляйте ПО.** Регулярно устанавливайте обновления операционной системы и приложений — они закрывают уязвимости.
- **Используйте надёжные пароли.** Создавайте сложные комбинации из букв, цифр и символов. Для разных сервисов — разные пароли. Рассмотрите использование менеджера паролей.
- **Включите двухфакторную аутентификацию** на всех важных аккаунтах (почта, соцсети, банкинг, «Госуслуги»).
- **Настройте уведомления о транзакциях.** Подключите SMS или push-уведомления по всем банковским картам и счетам.
- **Ограничьте видимость профиля в соцсетях.** Скройте номер телефона, дату рождения, место работы и другую чувствительную информацию от посторонних.
- **Будьте осторожны с публичным Wi-Fi.** Не вводите пароли и данные карт в общественных сетях без VPN.
- **Скачивайте приложения только из официальных магазинов** (Google Play, App Store).
- **Проверяйте разрешения приложений.** Не давайте доступ к камере, микрофону, контактам без необходимости.

## 4. Контролируйте финансовые операции

- **Установите лимиты:**
  - на сумму одной покупки;
  - на количество операций за день/месяц;
  - на отдельные типы транзакций (переводы физлицам, онлайн-платежи).

- **Регулярно проверяйте выписки** по счетам и картам. Обращайте внимание на подозрительные списания.
- **Блокируйте карту сразу** при потере или подозрении на компрометацию.
- **Не храните все деньги на одной карте.** Распределите средства между несколькими счетами.
- **Используйте виртуальные карты** для онлайн-покупок с ограниченным лимитом.

## 5. Развивайте критическое мышление

- **Проверяйте информацию.** Если предложение кажется слишком выгодным, скорее всего, это обман. Ищите подтверждения на официальных сайтах, в СМИ.
- **Обсуждайте сомнительные ситуации** с близкими. Второй взгляд помогает заметить то, что вы могли упустить.
- **Изучайте основы кибербезопасности.** Проходите бесплатные курсы, читайте статьи от банков и регуляторов.
- **Будьте скептичны к неожиданным «подаркам» и «выигрышам».** Если вы не участвовали в акции, выиграть невозможно.
- **Помните:** никто не имеет права принуждать вас к быстрому решению. Всегда берите паузу, чтобы всё обдумать.

## 6. Обратите внимание на тревожные сигналы

Поводом насторожиться могут быть:

- неожиданные звонки или сообщения о подозрительных операциях по счёту;
- странные списания со счёта;
- невозможность войти в онлайн-банк или почту;
- появление незнакомых программ на устройстве;
- сообщения от друзей о том, что с вашего аккаунта рассылают просьбы о деньгах.

**Что делать:**

- Сохраняйте спокойствие.
- Проверьте информацию через официальные каналы (звонок в банк по номеру с карты, личный визит в отделение).
- Сообщите о подозрительной активности в службу поддержки сервиса.

## 7. Что делать, если вы стали жертвой мошенников

**Экстренные меры:**

1. **Прервите общение** с мошенниками. Не отвечайте на звонки и сообщения.

2. **Заблокируйте карты и счета**, с которых были списаны деньги.
3. **Смените пароли** от онлайн-банка, почты, соцсетей.
4. **Сообщите в банк** о мошеннической операции. Подайте заявление о несогласии с операцией — у вас есть право на возврат средств в ряде случаев.
5. **Обратитесь в полицию** и подайте заявление о мошенничестве. Приложите все доказательства: скриншоты переписки, выписки по счёту, записи разговоров.
6. **Проведите проверку устройства** на вирусы. При необходимости сбросьте настройки до заводских.
7. **Предупредите близких** — мошенники могут использовать ваши контакты для новых атак.

**После экстренных мер:**

- Проанализируйте ситуацию: что стало точкой входа для мошенников (какой звонок, сообщение, сайт).
- Усильте защиту аккаунтов: включите двухфакторную аутентификацию, обновите пароли.
- При необходимости обратитесь к юристу для консультации по дальнейшим действиям.

**Важно:**

- Технические средства (антивирусы, фильтры спама) помогают, но не заменяют бдительности и критического мышления.
- Регулярно обновляйте знания о новых схемах мошенничества — преступники постоянно придумывают новые способы обмана.
- Делитесь опытом с близкими — предупреждённый человек меньше рискует стать жертвой.