Муниципальное бюджетное общеобразовательное
учреждение «Средняя общеобразовательная школа №1»

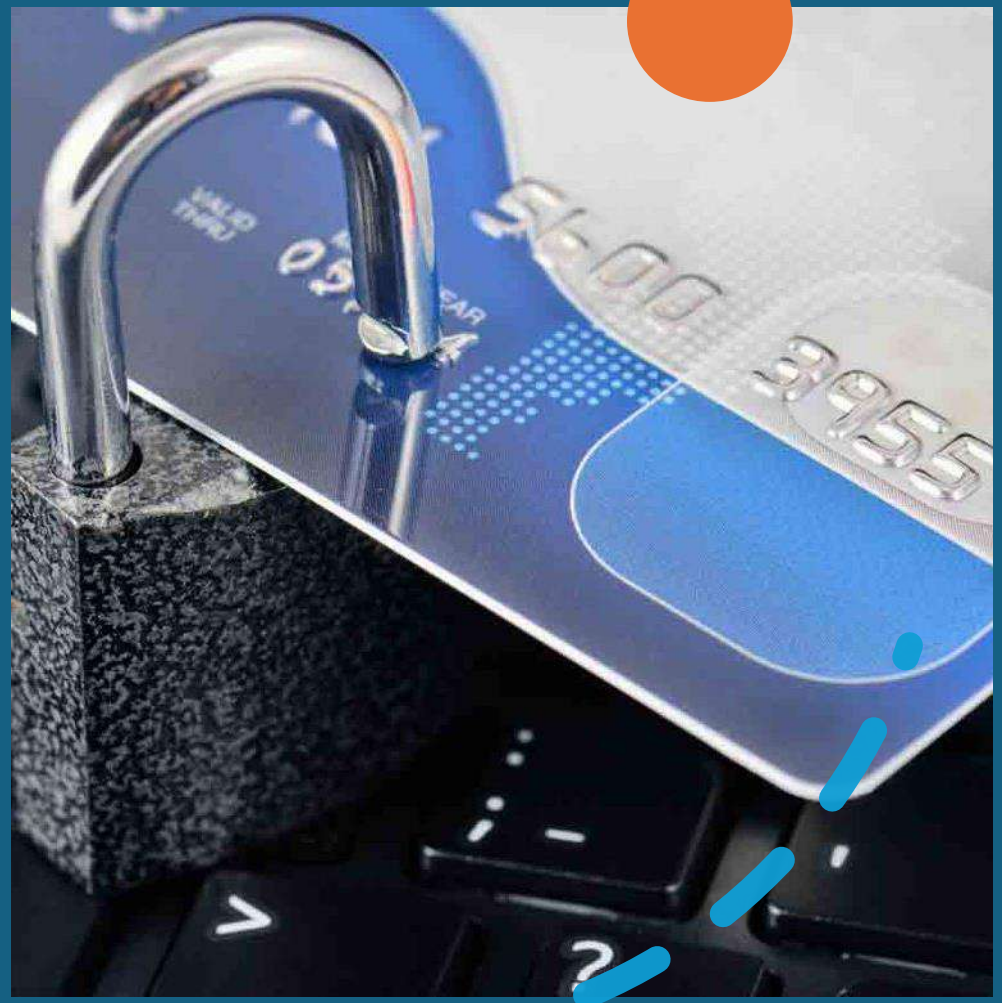
Цифровой кошелек: как сохранить его в безопасности

Выполнила ученица 11 "А" класса
МБОУ СОШ №1
Курбонова Нозияхон Хукмиддиновна

Междуреченск 2025 г

Что такое цифровой кошелек и почему его нужно защищать?

Цифровой кошелёк (электронный кошелёк) — это онлайн-сервис для хранения и использования денег в цифровом формате. По сути, это виртуальный счёт, доступ к которому осуществляется через сайт или мобильное приложение.



- ***Что хранится в цифровом кошельке:***
  - Банковские карты и реквизиты
  - Электронные деньги (QIWI, Яндекс.Деньги)
  - Криптовалюты (Bitcoin, Ethereum)
  - Цифровые документы и удостоверения
  - Бонусные карты и проездные
- ***Почему это привлекает мошенников:***
  - Прямой доступ к вашим деньгам
  - Возможность быстрого перевода средств
  - Сложность отслеживания операций
  - Анонимность преступников

Основные угрозы для вашего кошелька

1.Фишинг и мошеннические сайты

- Поддельные приложения кошельков
- Фейковые письма от "службы поддержки"
- Клоны официальных сайтов

2.Вредоносное ПО

- Кейлоггеры (перехват ввода)
- Трояны для мобильных устройств
- Шпионское программное обеспечение

3.Социальная инженерия

- Звонки от "сотрудников банка"
- СМС с просьбой перевести деньги
- Поддельные уведомления о блокировке

Создание надежного фундамента безопасности

- ***Выбор безопасного кошелька:***
  - Проверяйте репутацию разработчика
  - Изучайте отзывы и рейтинги
  - Скачивайте только из официальных магазинов приложений
- ***Создание мощного пароля:***
  - Минимум 12 символов
  - Комбинация букв (заглавных и строчных), цифр, специальных символов
  - Уникальный пароль для каждого сервиса
  - Пример надежного пароля: "M0сква#2024$Вечер!"
- ***Двухфакторная аутентификация (2FA):***
  Двухфакторная аутентификация (2FA) — метод защиты доступа к системам и данным, при котором для входа требуется подтверждение личности с использованием двух разных факторов. Обычно первый фактор — пароль, а второй может быть кодом из SMS, push-уведомлением, биометрией или аппаратным ключом.
- ***Цель 2FA*** — повысить уровень безопасности, так как одной лишь комбинации логина и пароля часто недостаточно для защиты конфиденциальной информации. Пароли могут взломать или украсть, но если к этому добавлен второй фактор, то даже при утечке пароля доступ к учётной записи останется защищённым.

Секретная фраза (Seed) — золотой ключ от вашего кошелька

Seed-фраза — это последовательность из 12, 18 или 24 слов, которая служит главным инструментом для восстановления доступа к криптовалютному кошельку.

- ***Правила хранения:***
  - ☑ Никогда не храните в цифровом виде
  - ☑ Не делайте скриншоты
  - ☑ Не отправляйте по интернету
  - ☑ Записывайте на бумаге или металлической пластине

- ***Чего никогда нельзя делать***:
  - ☑ Не передавайте никому
  - ☑ Не вводите на подозрительных сайтах
  - ☑ Не храните вместе с устройством
  - ☑ Не теряйте — это невосстановимо

Ежедневные привычки для безопасности

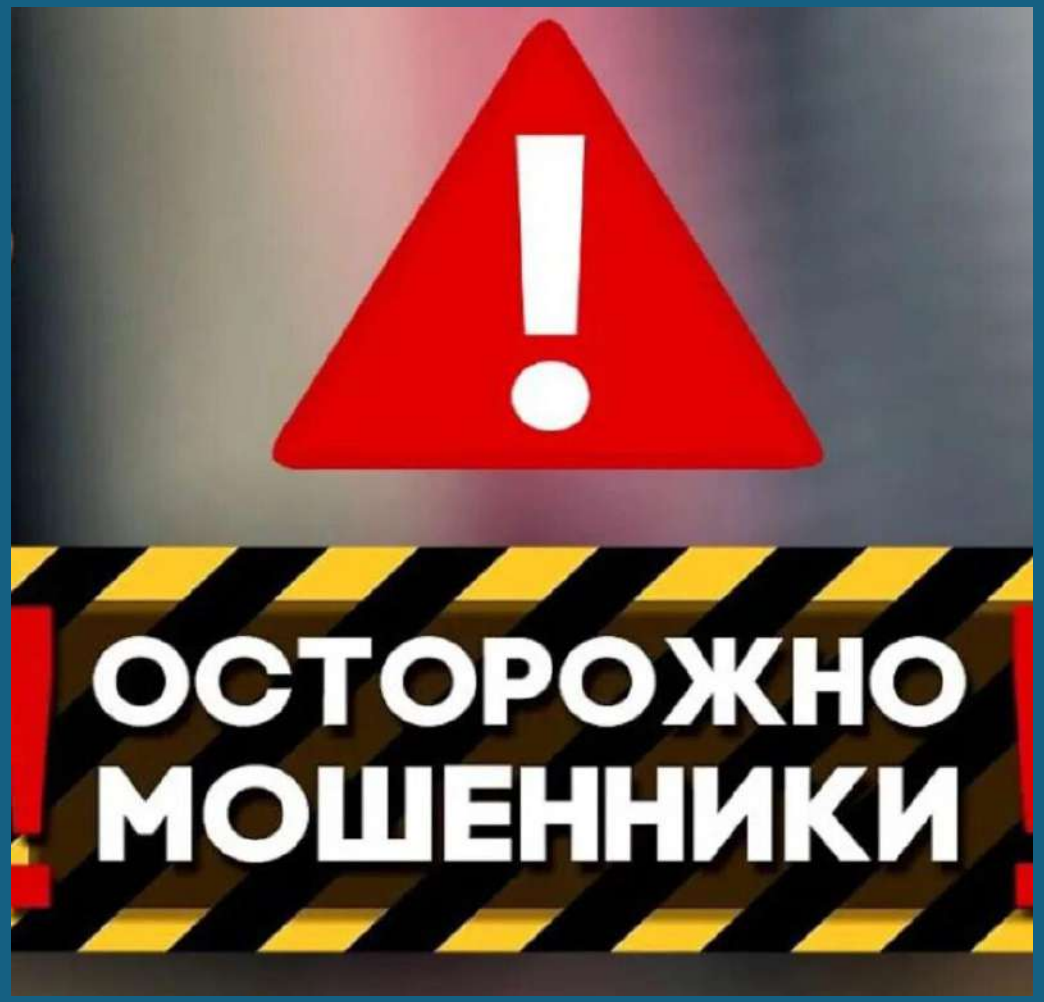
❖ ***Работа с устройствами:***
- Всегда используйте блокировку экрана
- Регулярно обновляйте ОС и приложения
- Устанавливайте антивирусное ПО
- Делайте резервные копии важных данных

❖ ***Финансовые операции:***
- Проверяйте адрес сайта перед вводом данных
- Не используйте публичный Wi-Fi для платежей
- Включайте уведомления о всех операциях
- Регулярно проверяйте историю транзакций

❖ ***Личная бдительность:***
- Никому не сообщайте коды из СМС
- Проверяйте отправителя писем и сообщений
- Не торопитесь — мошенники создают искусственную срочность

Как распознать мошенников?

- ✓ ***Подозрительные сообщения:***
  - "Ваш кошелек заблокирован"
  - "Срочно обновите данные"
  - "Вы выиграли приз — оплатите доставку"
- ✓ ***Признаки фишинговых сайтов:***
  - Опечатки в названии сайта
  - Отсутствие HTTPS в адресе
  - Некачественный дизайн
  - Требуют ввести Seed-фразу
- ✓ ***Подозрительные действия:***
  - Звонок с неизвестного номера
  - Просьба установить "специальное" приложение
  - Требование срочно перевести деньги



Что делать при подозрении на взлом?

- ✓ ***Немедленные действия:***

  1.Переведите средства на резервный кошелек

  2.Заблокируйте текущий кошелек через поддержку

  3.Отзовите все выданные разрешения

  4.Смените все пароли и PIN-коды

- ✓ ***Восстановление безопасности:***

  1. Восстановите кошелек на новом устройстве с помощью Seed-фразы
  2.Проверьте все устройства на наличие вирусов
  3. Установите дополнительные средства защиты

- ✓ ***Юридические действия:***

  1. Сообщите в правоохранительные органы
  2.Обратитесь в службу поддержки кошелька
  3.Сообщите в банк, если затронуты карты

Дополнительные инструменты защиты

► ***Аппаратные кошельки:***

Ledger, Trezor —производители аппаратных кошельков для криптовалют.

➢ ***Хранение ключей оффлайн***
- Подтверждение операций на устройстве

➢ ***Программные решения:***
- Менеджеры паролей (LastPass, 1Password)
- Антивирусы с защитой от фишинга
- VPN для безопасного соединения

➢ ***Организационные меры:***
- Разделение кошельков по назначению
- Установление лимитов на операции
- Регулярный аудит безопасности

Итоги и начало вашей безопасности

❖ ***Главные правила, которые нужно запомнить:***

1.Seed-фраза — священна, храните только оффлайн.

2.Двухфакторная аутентификация обязательна везде.

3.Обновления — это исправления уязвимостей.

4.Доверяй, но проверяй — всегда!

❖ ***План действий на сегодня:***

1. Проверить настройки безопасности всех кошельков.
2.Включить 2FA везде, где это возможно.
3.Обновить пароли на более сложные.
4.Сохранить Seed-фразу в надежном месте.

Ваша финансовая безопасность начинается сегодня!