Девятый этап Всероссийской просветительской Эстафеты «Мои финансы»

МИНФИН РОССИИ

мои финансы

Безопасность денег в цифровой среде

спикер,
должность спикера

ЦИФРОВЫЕ ДЕНЬГИ

Цифровые деньги – это не единое явление, а сложная экосистема, в которой сочетаются разные технологические и институциональные модели

БАНКОВСКИЕ КАРТЫ И ОНЛАЙН-БАНКИНГ

Банковская карта – это инструмент доступа к счету, который позволяет распоряжаться деньгами

Онлайн-банкинг - это цифровой интерфейс управления этим счетом

Преимущества:

- высокая скорость операций
- удобство
- интеграция с другими сервисами

Важно: даже самая защищенная система становится уязвимой, если пользователь сам инициирует перевод злоумышленнику

ЦИФРОВАЯ ВАЛЮТА (ЦИФРОВОЙ РУБЛЬ)

- **это третья форма национальной валюты, уникальный цифровой код, выпускаемый и хранящийся на балансе Банка России**

Польза для граждан:

- Доступ к цифровому кошельку через любой банк
- Снижение издержек на переводы
- Безопасность
- Снижение кредитного риска

Польза для бизнеса:

- Снижение издержек на переводы
- Повышение прозрачности
- Контроль за денежными потоками

Польза для государства:

- Повышение эффективности бюджетного процесса
- Борьба с мошенничеством
- Ускорение межбюджетных трансфертов
- Экономия государственного бюджета

Проблема:

приватность, потенциальный тотальный контроль транзакций, концентрация рисков в одной системе, сокращение объёма кредитных денег в экономике

ЭЛЕКТРОННЫЙ КОШЕЛЁК

– это виртуальный счёт, на котором хранятся деньги в электронном виде, доступ осуществляется через сайт или мобильное приложение

Контроль:
Федеральный закон №161-ФЗ
«О национальной платёжной системе»

Преимущества:
упрощенная регистрация и быстрый доступ к платежам

ВИДЫ:

- **Анонимный**
- **Именной**
- **Идентифицированный**

Но: Упрощенные процедуры идентификации – источник риска!

КРИПТОВАЛЮТА

– это децентрализованные цифровые активы, основанные на технологии блокчейн

В России: запрет на использование криптовалют для оплаты товаров и услуг внутри страны (ФЗ от 31 июля 2020 года №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»)

Особенности криптовалют:

- отсутствие централизованного контроля
- необратимость транзакций
- повышенная ответственность пользователя за сохранность средств

Риски:

- безвозвратная потеря средств
- мошенничество
- высокая волатильность

Важно: отсутствие государственных гарантий

ВИРТУАЛЬНАЯ ИГРОВАЯ ВАЛЮТА

- **это особая форма цифровых активов, существующая в рамках онлайн-игр и игровых платформ, которая может зарабатываться в игре или покупаться за реальные деньги**

Важно: пользователь не владеет валютой, а только использует её по правилам платформы

На **вторичных рынках** виртуальные активы приобретают денежную оценку

В **массовых многопользовательских играх и платформах** с пользовательским контентом появляются полноценные внутриигровые экономики

УГРОЗЫ: МОШЕННИЧЕСТВО

- это совокупность противоправных действий, направленных на незаконное завладение финансовыми средствами или конфиденциальной информацией пользователей посредством обмана и злоупотребления доверием

Особенность:

- сочетает технические инструменты с методами социальной инженерии

Механизмы:

- вызывают у жертвы страх, панику из-за срочности, доверия или жадности

Риски:

- финансовые потери
- подрыв доверия к цифровым финансовым инструментам
- психологический ущерб

Современные мошеннические схемы адаптируются под конкретную аудиторию

УГРОЗЫ: ФИШИНГ

- это метод получения конфиденциальной информации путем создания поддельных сайтов или сообщений, имитирующих легитимные сервисы

Примеры:

- доменные имена, отличающиеся одной-двумя буквами
- внедрение SSL-сертификатов
- копирование дизайна, структуры и функциональности интерфейса

Риски:

- хищение денежных средств
- компрометация учетных записей
- утечка персональных данных
- возможность последующих атак с использованием полученной информации

Развитие ИИ → генерирование текста под конкретную аудиторию/ создание убедительных видео- и аудиоматериалы/опасные QR-коды

УГРОЗЫ: ДИПФЕЙКИ

- это использование технологий ИИ для создания синтетических аудио- и видеоматериалов, имитирующих реальных людей

Примеры сценариев мошенничества:

- «звонок» от руководителя с просьбой срочно пройти по сомнительной ссылке или назвать код из смс
- видеообращение знакомого с просьбой о помощи
- поддельные интервью и заявления
- голосовые сообщения, имитирующие близких

Риски:

- финансовый ущерб
- подрыв доверия к цифровым коммуникациям
- репутационные потери

Дипфейки размывают границу между подлинным и искусственным контентом

УГРОЗЫ: РИСКИ В СОЦИАЛЬНЫХ СЕТЯХ И ИГРАХ

В онлайн-играх (особенно на вторичных рынках) нет правовой защиты

Типичные риски:

- взлом аккаунтов
- фальшивые розыгрыши
- мошеннические «скины» и внутриигровые предметы

Механизм атак:

- сбор информации о потенциальной жертве
- взлом учетной записи или создание поддельного профиля
- побуждение к переводу средств или передаче данных

Последствия:

- потеря виртуальных активов
- утрата доступа к аккаунту
- потеря реальных денег при покупках на поддельных торговых площадках или оплате услуг мошенников
- заражение компьютера вредоносным ПО

ПАРОЛИ И ДОСТУПЫ

Пароли – это первичный и наиболее распространенный инструмент аутентификации

Передача кода третьим лицам = добровольное разрешение на проведение операции

Человеческий фактор:

- простые и легко запоминающиеся комбинации
- один пароль на все ресурсы
- хранение «шпаргалок» с паролями в небезопасных местах

Помогает:

- двухфакторная аутентификация (получаем код для подтверждения операции)
- биометрические методы аутентификации (проблема – дипфейки)

Рекомендуется:

- использовать уникальные пароли для каждого сервиса
- создавать сложные комбинации (длина не менее 12 символов)
- применять менеджеры паролей
- включать двухфакторную аутентификацию

БЕЗОПАСНОСТЬ УСТРОЙСТВ

Угроза:

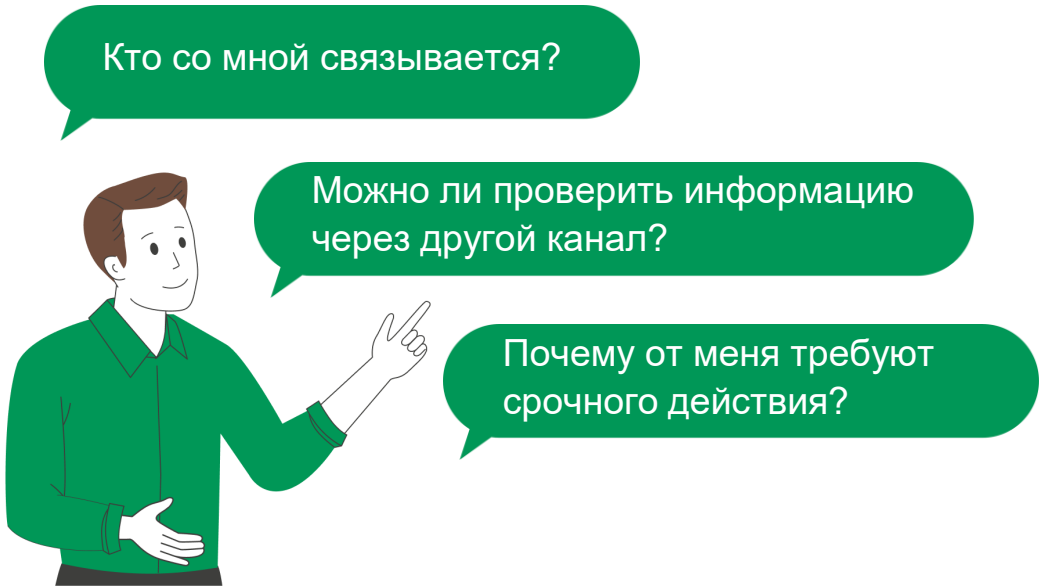
- вредоносные приложения
- поддельные версии банковских программ
- трояны, перехватывающие СМС

Необходимо:

- регулярно обновлять ОС
- устанавливать приложения из официальных источников
- использовать антивирусное ПО
- избегать подключения к открытым Wi-Fi-сетям

ПОВЕДЕНИЕ В ИНТЕРНЕТЕ

Если возникает давление или срочность – это почти всегда признак мошенничества



Вопросы себе

Ключевые правила:

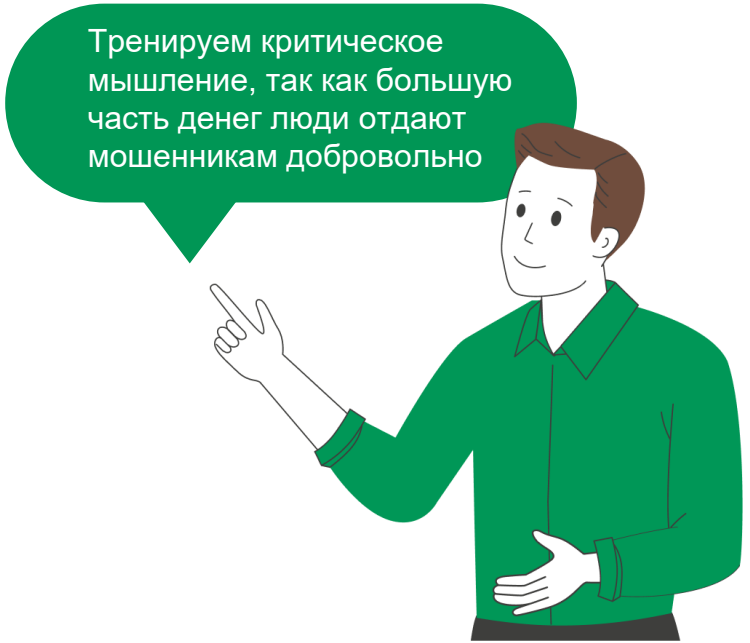
- не переходить по подозрительным ссылкам
- внимательно проверять адрес сайта
- не сообщать коды из СМС и пуш-уведомлений
- не доверять сообщениям, вызывающим панику или срочность

РАБОТА С ДЕНЬГАМИ

Если возникает давление или срочность – это почти всегда признак мошенничества

Дополнительные меры безопасности:

- установка лимитов на операции
- подключение уведомлений о транзакциях
- запрет на онлайн-кредиты без подтверждения
- использование отдельных карт для онлайн-покупок
- разделение финансовых потоков



Мини-игра «Распознаешь мошенника?»

МИНИ-ИГРА «РАСПОЗНАЕШЬ МОШЕННИКА?»

1. Вам пишет друг в мессенджере: «Скинь срочно денег, потом объясню»
2. Приходит СМС от банка с кодом, хотя вы ничего не делали и не запрашивали подтверждение операции
3. Вам звонит человек, представляется сотрудником службы безопасности банка и говорит: «С вашего счета пытаются списать деньги, нужно срочно перевести их на безопасный счет»
4. Сайт выглядит как известный магазин, но адрес отличается одной буквой
5. Вам предлагают вложиться в криптовалюту с гарантированной доходностью 50% в месяц
6. Одноклассник присылает голосовое сообщение с просьбой сделать срочный перевод
7. После публикации жалобы в соцсети вам пишет «служба поддержки» и просит данные карты для возврата денег
8. Приходит письмо на почту: «Вы обязаны срочно оплатить штраф. Перейдите по ссылке, иначе будет возбуждено дело»
9. Вам предлагают купить игровую валюту в популярной онлайн-игре в 2 раза дешевле, чем в официальном магазине, с переводом на карту

ЗАКЛЮЧЕНИЕ

Цифровая грамотность + **Критическое мышление** + **Соблюдение базовых правил безопасности** = **УСПЕХ!**

В цифровой экономике безопасность денег определяется **не только технологиями, но и качеством решений,** которые принимает сам пользователь

Больше полезной информации можно найти

на портале моифинансы.рф и в социальных сетях