

## Цифровая финансовая безопасность семьи: о чем нужно знать

*О важных правилах семейной финансовой безопасности в [интервью «Газета.ру»](#) рассказал эксперт проекта НИФИ Минфина России «Моифинансы.рф» Дмитрий Модель.*

### 1. Пароль, который не подберут: правила создания и срок жизни

Надежный пароль должен быть длинным, уникальным для каждого сервиса и не содержать личных данных вроде имен или дат рождения. Запомнить десятки таких комбинаций невозможно — здесь на помощь приходит менеджер паролей. Это специальная программа, которая генерирует сложные пароли, хранит их в зашифрованном хранилище и автоматически подставляет при входе на сайты и в приложения. Вам нужно помнить только один мастер-пароль, открывающий доступ к этому цифровому сейфу. Это намного безопаснее, чем держать пароли в записках телефона или пересылать в семейных чатах. Менять пароли без повода не нужно: современные стандарты безопасности рекомендуют смену только при подозрении на компрометацию, а не по календарю. Единственное, что нельзя менять годами, — принцип «один сервис — один пароль», и менеджер паролей делает его соблюдение простым и удобным.

### 2. Старшее поколение: «вторая рука», самозапреты и разговор вместо лекции

Люди старшего возраста чаще попадают на уловки не из-за доверчивости, а оттого, что мошенники бьют в самое больное — страх за близких и одиночество. Поэтому главная защита — не техническая инструкция, а постоянный контакт. Проблемы случаются там, где общение сводится к минимуму.

С практической стороны: во многие банковские приложения сейчас можно подключить «вторую руку» — официальный сервис, при котором доверенный родственник видит уведомления о крупных операциях и может вовремя остановить сомнительный перевод, не имея полного доступа к счету. Другой мощный инструмент — самозапреты на портале Госуслуг. Они позволяют ограничить оформление кредитов, сделок с недвижимостью или выдачу новых сим-карт без личного присутствия. Это особенно важно для старших родственников, чьи персональные данные могли утечь к мошенникам. Настройте оба механизма вместе с родителями, бабушками и дедушками, объяснив, что это не отбирает у них самостоятельность, а просто ставит дополнительный барьер для злоумышленников.

### 3. Кодовое слово: почему это не просто игра, а реальный инструмент безопасности

Кодовое слово — это семейный пароль, секрет, известный только самым близким. Его главная задача — подтвердить личность в критической ситуации, когда времени на размышления нет, а ставки высоки. Сегодня мошенники научились подделывать голос

и даже видео с помощью дипфейков: вам могут позвонить «голосом сына» или «с лицом внучки» и сообщить, что они попали в ДТП, нуждаются в срочной операции или требуют залог за освобождение. В такой момент паника отключает логику, и единственный способ мгновенно отличить реального близкого от имитации — задать вопрос, ответ на который знают только свои.

Кодовое слово работает универсально в любом тревожном сценарии:

- звонок от имени родственника с просьбой срочно перевести деньги («Мама, я сбил человека»);
- дипфейк-видеосообщение или голосовое сообщение с подделанным голосом;
- звонок от якобы сотрудника полиции или больницы, который торопит и давит на эмоции;
- попытка получить доступ к аккаунтам или устройствам под видом «помощи» от члена семьи.

Правило простое: договоритесь о кодовом слове сегодня. Это не должны быть данные, которые можно найти в соцсетях, — кличка питомца, дата рождения, девичья фамилия. Идеальный вариант — короткая, неочевидная фраза или слово, имеющее значение только для вашего семейного круга. Если человек на том конце провода не может его назвать — немедленно кладите трубку, кем бы он ни представлялся.

#### 4. Пуш-уведомления: ваша сигнализация по всем картам

Перед крупной кражей мошенники почти всегда тестируют карту парой мелких списаний. Если у вас не настроены СМС или пуш-уведомления о каждой операции, вы рискуете пропустить сигнал тревоги. Подключите уведомления на карты всех членов семьи, включая детские и пенсионные, — это пять минут в приложении, которые могут спасти накопления.

#### 5. Двухфакторная аутентификация: второй замок там, где это возможно

Пароль можно подсмотреть или украсть. Второй фактор защиты (одноразовый код) не даст зайти в аккаунт, даже если пароль утечет. Включите двухфакторную аутентификацию везде, где она есть: Госуслуги, мессенджеры, почта, маркетплейсы. Самый безопасный вариант — приложение-аутентификатор, генерирующее коды на устройстве; оно надежнее, чем СМС, которые можно перехватить.

#### 6. Дропперство: когда «легкий заработок» делает соучастником преступления

Одна из самых опасных ловушек, в которую сегодня активно затягивают и детей, подростков, и людей старшего возраста, — участие в схемах по выводу и обналичиванию похищенных денег. Таких подставных лиц называют дропперами (или дропами). Ими становятся те, кто за вознаграждение передает посторонним доступ к

своей банковской карте, оформляет карту на свое имя для других людей или сам совершает переводы по чужой указке. По данным Росфинмониторинга, в 2025 году общее число дропперов достигло примерно 800 тыс. человек, из них около 272 тыс. — несовершеннолетние, и их количество выросло на 10% за год.

Многие жертвы искренне не понимают, что становятся соучастниками преступления. Мошенники играют на желании быстро и легко заработать, особенно у подростков и людей с низкой финансовой грамотностью. Объявления о «вакансиях» распространяют через Telegram-каналы, соцсети, игровые чаты и даже Discord. Типичные легенды: «помощник по платежам», «удаленная работа без опыта» или «посредник для обхода санкций» — а на деле через человека просто прогоняют украденные деньги.

С июля 2025 года в России введена уголовная ответственность для дропперов по ст. 187 УК РФ. За передачу карты или доступа к счету посторонним, а также за операции по чужому указанию можно получить до трех лет лишения свободы, а за покупку чужих карт для вывода похищенных средств — до шести лет. Уголовная ответственность наступает с 16 лет, а для тех, кто младше, — административная с обязанностью возместить ущерб. Кроме судимости, дроппер рискует навсегда попасть в черный список банков: счета и карты блокируются, открыть новые становится практически невозможно.

Ключевое правило безопасности для всей семьи: никогда, никому и ни за какие деньги не передавайте свои банковские карты, доступ к личному кабинету и не совершайте переводы по просьбе незнакомцев — даже если это выглядит как безобидная «помощь с платежами» или «тестовое задание». Помните: анонимность в сети — иллюзия, все операции отслеживаются, и одно необдуманное действие действительно может обернуться серьезными последствиями.

## **ВАЖНО!**

**Главное семейное правило: мошенники играют на спешке и эмоциях.**

В любой тревожной ситуации — пауза, звонок близким и проверка через официальные каналы. Быть на связи друг с другом — самая надежная защита для всей семьи от цифровых угроз.