Защита от мошенников (сохранение собственных средств). Работают базовые принципы безопасности.

Никому не сообщать конфиденциальные данные. Нельзя передавать третьим лицам коды из СМС, CVC-коды с обратной стороны карты, логины и пароли от онлайн-банкинга. Сотрудники банков, правоохранительных органов, Росфинмониторинга никогда не запрашивают эту информацию.

Критическое отношение к звонкам «из банка» или госорганов. Современные преступники используют методы психологической атаки: если собеседник торопит, пугает блокировкой счетов или требует перевести деньги на «безопасный счет», разговор нужно немедленно прекратить и самостоятельно перезвонить в банк по официальному номеру, СООБЩИТЬ РОДИТЕЛЯМ, СПРОСИТЬ, УВЕДОМИТЬ. ***НЕ ДЕЙСТОВОВАТЬ В ОДИНОЧКУ.***

Защита пожилых родственников. Необходимо заранее объяснить им алгоритм действий: при любых подозрительных звонках они должны класть трубку и связываться с близкими для консультации.

Как не стать соучастником преступления (дроппером)

Дропперство — это передача своей банковской карты, счета или использование своих данных для перевода грязных денег за вознаграждение. С июля 2025 года в России введена уголовная ответственность за эти действия (до шести лет лишения свободы), а база ЦБ РФ уже содержит более двух миллионов молодых людей, вовлеченных в такие схемы. ***Дропперство редко ограничивается только переводом похищенных пенсий — оно часто становится первым шагом к вовлечению молодежи в тяжкие преступления, включая финансирвование экстремизма и терроризма.***

Никогда не передавать свои банковские карты третьим лицам. Даже если предлагают «легкий заработок» за перевод пары сумм, владелец карты становится соучастником отмывания денег или другого преступления. Ответственность за это предусмотрена УК РФ. ***Не привязывать чужие номера к своим картам.*** Мошенники часто просят школьников или студентов привязать их телефонный номер к карте родителей или самого студента для подтверждения операций. Это прямой путь к статусу дроппера.

Стратегический подход к безопасности

Для личной безопасности каждого гражданина главным правилом остается осознание ответственности: ***«Ответственность за все операции, совершаемые с использованием ваших банковских карт или счетов, несёте только вы».***

Любое предложение передать карту или доступ к счету другому человеку должно восприниматься как попытка сделать вас крайним в уголовном деле.

Типовые сценарии и банальные примеры

Органы внутренних дел регулярно публикуют сводки с идентичными механиками вовлечения:

Механика	Описание
«Ошибочный перевод»	На карту подростка приходят деньги от неизвестного лица. Ему пишут или звонят с просьбой вернуть сумму, но указывают другой номер телефона или счет. Как только подросток делает перевод со своей карты, он становится частью цепочки по отмыванию похищенных средств. Полиция подчеркивает: самостоятельно возвращать такие деньги нельзя, нужно обращаться в банк.
«Оплата виртуальных предметов»	Мошенники находят жертв в онлайн-играх (Roblox, Minecraft, CS2). Они предлагают купить внутриигровой предмет или валюту дешевле рыночной цены. Для оплаты дают реквизиты банковской карты реального человека (дропа/подростка). Деньги моментально выводятся, а покупатель остается ни с чем.
Сеть одноклассников	Получив первую выплату (обычно 300–500 рублей), подросток начинает искать новых участников среди друзей и одноклассников, создавая локальную сеть дропперов ради процента от оборота. Это часто заканчивается групповыми задержаниями целого класса.
«Тайный сотрудник банка / ФСБ»	Подростку пишет якобы представитель госорганов или службы безопасности банка через мессенджер. Просит провести «тестовый платеж» или «заблокировать подозрительный перевод», продиктовав данные карты или совершив операцию. Сотрудники полиции и спецслужб никогда не связываются с гражданами через Telegram или другие мессенджеры для перевода денег.