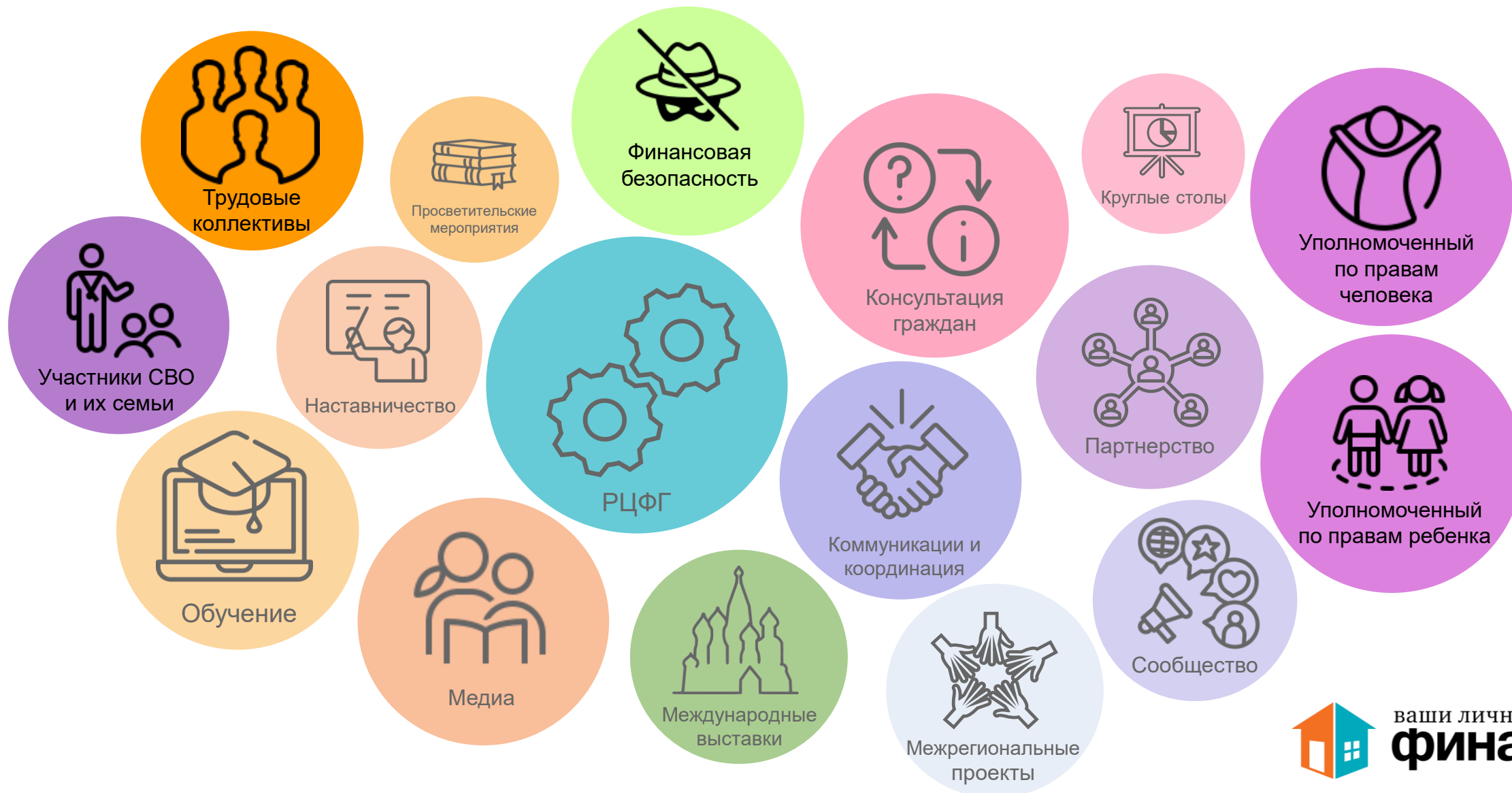


«От безопасности к успеху:
траектория молодежи
на пути к финансовой
культуре и благополучию»

Кудрявцева Оксана,
руководитель РЦФГ



Реализация программы ФГ



Г Викторина



Финансовое мошенничество — это противоправные действия в сфере денежного обращения, основанные на обмане, злоупотреблении доверием и других манипуляциях, с целью незаконного обогащения.

Цель мошенника — завладеть деньгами жертвы:

1

заставить перевести на счет или передать через курьера, обманом вынудить взять кредит

2

получить доступ к персональным и платежным данным и с их помощью украсть деньги

Социальная инженерия — основной метод мошенников. Это психологическое манипулирование человеком с целью заставить его выполнить определенные действия.



Мошенники действуют через

- телефон
- интернет и технические средства

Кибермошенники действуют через интернет и электронные устройства. Их цель — заставить жертву указать данные для входа в аккаунты, платежную информацию банковской карты.



Смишинг и вишинг — две разновидности фишинга. Смишинг происходит через СМС-сообщения, а вишинг через звонки.

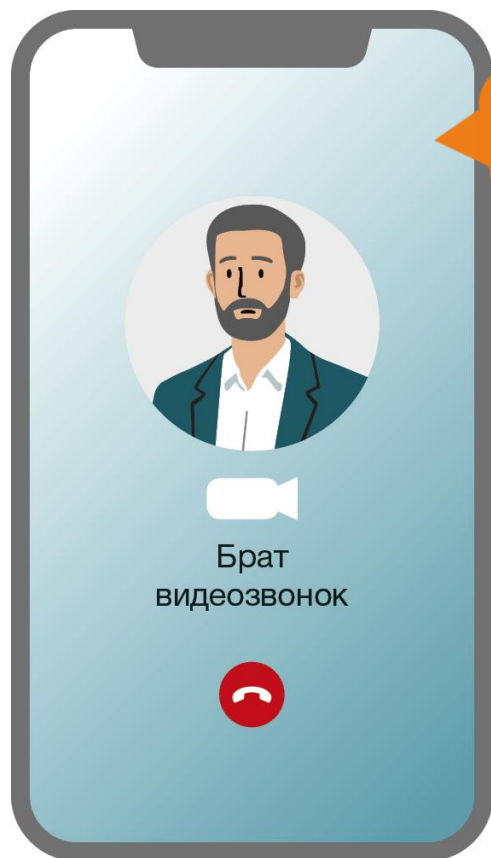
ФИШИНГ

Мошенники размещают рекламу о скидках от имени популярных интернет-магазинов, используя их фирменные цвета и стиль. Баннер ведет на фальшивую страницу магазина. Когда жертва вводит на ней данные карты, думая, что платит за товар, они попадают к мошенникам.



Защита:

- проверять информацию из объявлений в интернете
- проводить платежи только на проверенных ресурсах
- не оставлять платежные данные на сомнительных сайтах



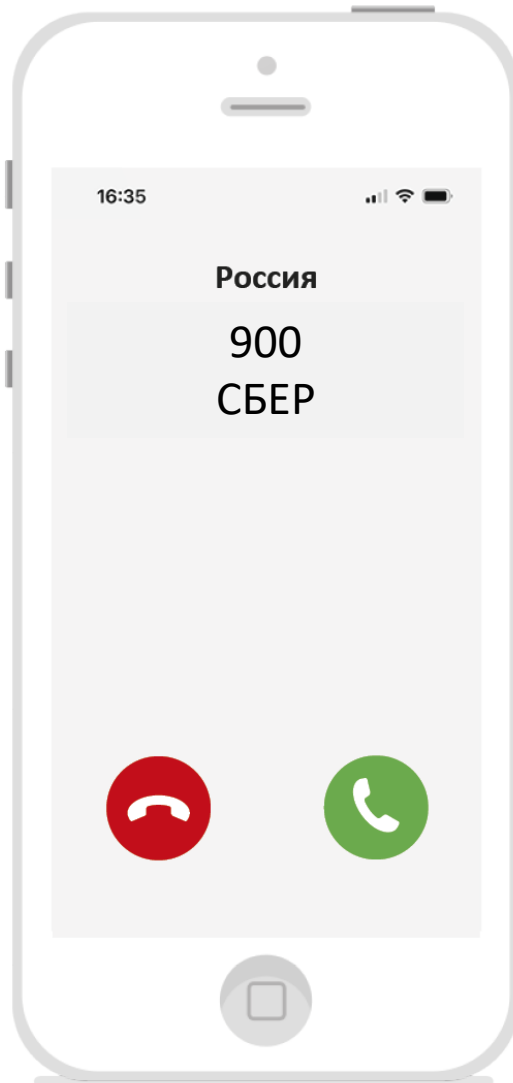
«Срочно нужно
переговорить с тобой,
связь плохая, напишу в
чате».

ДИПФЕЙКИ

Дипфейк — это правдоподобная имитация голоса, фото- или видеоизображения с помощью искусственного интеллекта. Для создания дипфейков мошенники используют фото и голосовые записи из взломанных аккаунтов, а затем от имени их владельцев рассылают сообщения, в которых просят деньги.

Защита:

- не выкладывать в общий доступ фото и видео, голосовые записи
- применять двухфакторную аутентификацию и надежные пароли в аккаунтах
- если кто-то знакомый просит перевести деньги, перезвонить и проверить информацию
- при оплате курсов блогеров и подписок обращать внимание на способ оплаты: в личных сообщениях ссылки на оплату высылают только мошенники



«Ваше приложение банка перестанет работать через 2 дня. Чтобы сохранить его, скачайте обновление по ссылке» ...

СПУФИНГ

Мошенники маскируются под других людей или компании через подмену номера телефона/электронного адреса, чтобы получить доступ к персональным данным, загрузить на устройство жертвы вредоносную программу или заставить отдать деньги.

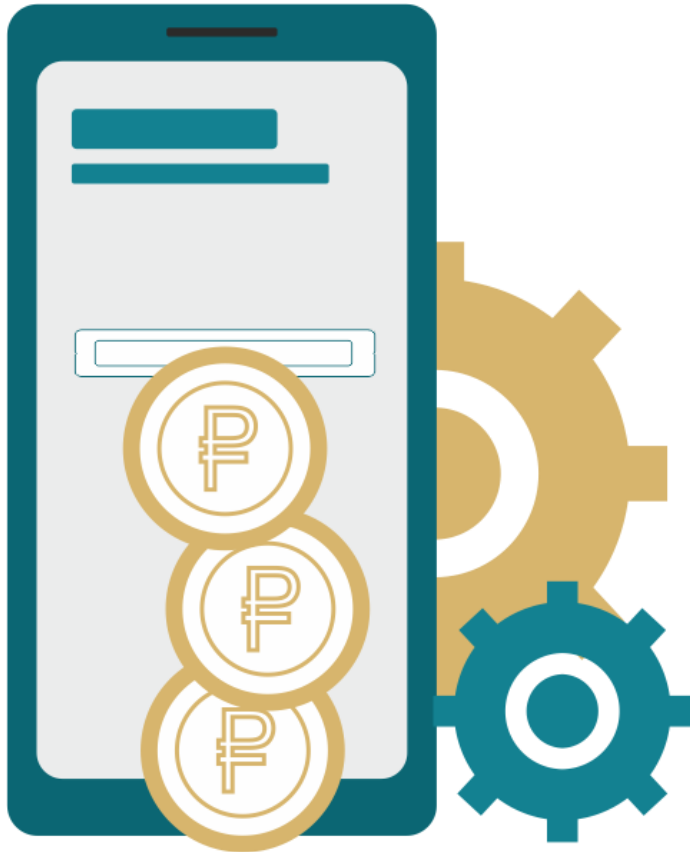
Защита:

- проверять информацию через официальные каналы организации, от имени которой звонили/писали
- скачивать программы, приложения и обновления только с официальных ресурсов
- не выполнять действия, которые вам диктуют по телефону незнакомые люди

Важно

- ▶ Старайтесь не размещать в соцсетях персональную информацию
- ▶ Установите 2-факторную аутентификацию (по всем аккаунтам и электронным почтам)
- ▶ Установите само/запреты (кредит, услуги связи, на действия с недвижимостью, на массовые звонки)
- ▶ Регулярно проверяйте свою кредитную историю
- ▶ Используйте сервис «Вторая рука» (назначение доверенного лица)
- ▶ Установите антиспам-приложения/определитель номера (банки, операторы сотовой связи)
- ▶ Установите антивирусные программы
- ▶ Устанавливайте надежные пароли
- ▶ Регулярно проверяйте движение денежных средств на счетах банковских карт
- ▶ Родительский контроль, настройки безопасности в мессенджерах
- ▶ Отдельная карта для покупок в интернете





ЛЕГКИЙ ЗАРАБОТОК В ИНТЕРНЕТЕ

Мошенники размещают объявления об удаленной несложной работе с высокой оплатой. «Для работы» просят по ссылке скачать и установить на смартфон приложение, которое на самом деле является вредоносной программой, считывающей логины и пароли, содержание СМС и пуш-сообщений.

Защита:

- критически относиться к объявлениям о «непыльной работе» в интернете, за которую хорошо платят
- не скачивать программы и приложения по сторонним ссылкам
- установить на смартфон и регулярно обновлять антивирус

Дропы — это посредники, через банковские карты которых деньги от жертв поступают к мошеннику. Цепочка переводов может быть длинной. Цель — скрыть конечного получателя.

Дропами люди становятся как сознательно (работают за вознаграждение), так и случайно — в результате обмана мошенниками.

СПЕЦИАЛИЗАЦИЯ ДРОПОВ

Заливщик

Получает через курьера наличные от мошенника, вносит их на свой счет в банке и переводит другим дропам.

Транзитник

Перечисляет деньги на другую карту или электронный кошелек, оставляя часть себе как вознаграждение.

Обнальщик

Снимает поступившие на карту деньги, оставляет часть себе как вознаграждение, остальное передает третьему лицу.

Универсал

Может выполнять любую из дроперских функций.



При выявлении нетипичных операций по картам и счетам лиц, информация о которых содержится в базе данных Банка России, банкам предлагается временно приостанавливать дистанционный доступ к управлению счетом. Это усложнит злоумышленникам вывод денег и повысит вероятность возврата их законному владельцу.

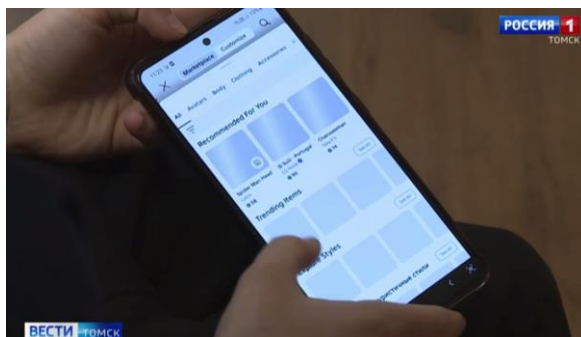
С 01.08.25 родители должны давать согласие на открытие счетов подростков и

имеют право получение выписки по счету ребенка с 01.07.26

Вся информация о мошенниках попадает в специальную базу, в том числе о дропах. При попадании в «черный список» через правоохранительные органы приостанавливается доступ к онлайн-банкингу и платежным картам.



Обман детей в играх



Дропы



Инструменты

Обучение педагогов/сотрудников образовательных учреждений: лекции, семинары, курсы

Открытые беседы с учащимися и онлайн-уроки совместно с правоохранительными органами

Совместные мероприятия: конкурс «Я.Финансы.Мир», квест «Изумрудный город», мини-фестивали, настольные и деловые игры

Цифровой журнал «ВЛФиник»



Готовые презентации



Подкасты



Видеоролики ШКИ



Сообщество педагогов

- Информация обо всех региональных и федеральных мероприятиях по финансовой грамотности: методических вебинарах, конференциях, конкурсах, играх, олимпиадах, фестивалях и т. п.
- Экспертная поддержка: возможность задать вопрос и получить квалифицированный ответ
- Прямая коммуникация с РЦФГ: запрос на методическую, организационную или иную помощь

- Возможность обмена опытом с коллегами



Г Как вовлечь детей



Интересная подача материала
(креатив: задания из журнала, подкасты, видеоролики, карточки)



Олимпиады по финансовой грамотности (в т. ч. перечневые), помощь
в подготовке



Верифицированные волонтерские часы
(в совместных мероприятиях с РЦФГ)

Информационные каналы РЦФГ Томской области

VLFin.ru

Портал финансовой
грамотности



Бесплатные консультации: 8-800-201-67-70



Оксана Кудрявцева

руководитель РЦФГ

тел. 8-800-201-6770, 716-797

