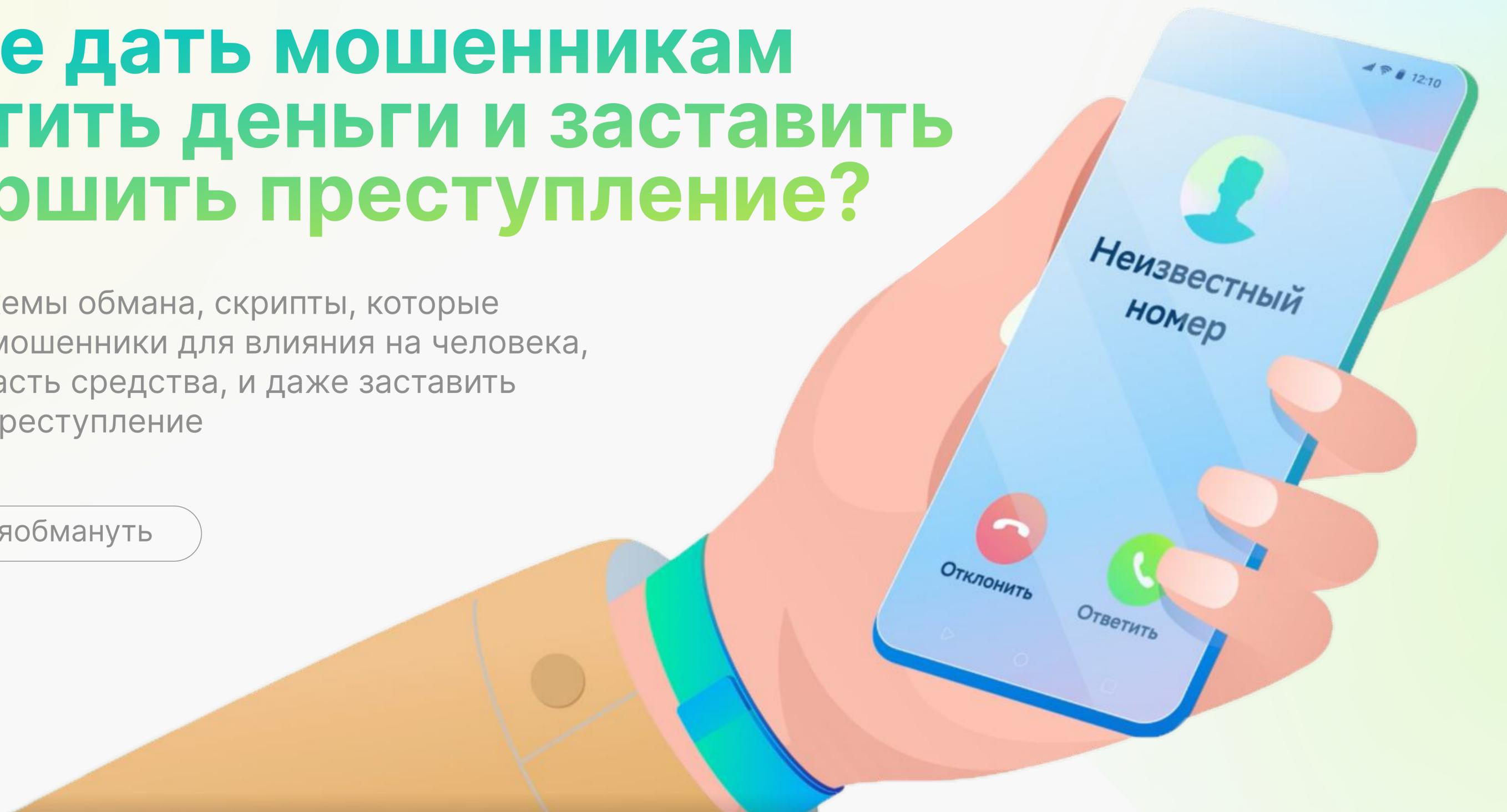




как не дать мошенникам похитить деньги и заставить совершить преступление?

Основные схемы обмана, скрипты, которые применяют мошенники для влияния на человека, с целью украсть средства, и даже заставить совершить преступление

#недайсебяобмануть



мошенники вынуждают «спасать» средства / имущество от лжемошенников

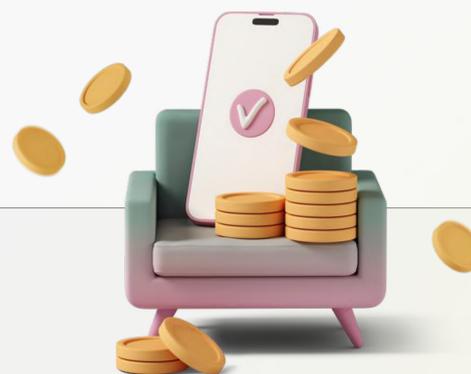
Какие схемы обмана используют?



возьмите встречный кредит для исчерпания кредитного лимита



переведите деньги на «безопасный счет»



продайте недвижимость по доверенности для предотвращения сделки



помогите поймать мошенников

Какие способы влияния?

Звонки, письма по электронной почте, в почтовый ящик, сообщения

- МВД, ФСБ, Следственный комитет
- Центральный банк РФ
- Служба безопасности банка
- Росфинмониторинг

Как защитить себя?

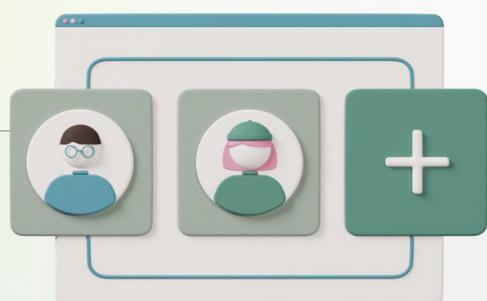
- 01** не сообщайте свои личные и банковские данные незнакомцам
- 02** не переходите по ссылкам из сообщений, удалите его и заблокируйте злоумышленника
- 03** не совершайте никаких действий и банковских операций по инструкциям звонящих
- 04** узнайте о состоянии средств, позвонив в контактный центр вашего банка, указанный на обороте карты, в онлайн приложении или отделении своего банка

помните, что сотрудники банков и государственных органов не звонят / не пишут в мессенджерах и не отправляют свои личные документы и не заставляют совершать нападения

- 05** сообщите о звонке/мошенничестве в свой банк (Сбербанк по номеру 900) и в полицию 112

мошенники похищают личные или банковские данные

Какие схемы обмана используют?



обновите личный кабинет / аккаунт



продлите договор



оформите выплату

Какие способы влияния?

Звонки, письма по электронной почте, в почтовый ящик, сообщения

- Гоуслуги
- МФЦ
- ПФР
- Сотовые операторы
- Министерство здравоохранения
- Социальные организации

Как защитить себя?

- 01** не сообщайте свои личные и банковские данные незнакомцам
- 02** не устанавливайте программы и приложения, удалите его и заблокируйте злоумышленника
- 03** узнайте о состоянии средств, позвонив в контактный центр вашего банка, указанный на обороте карты, в онлайн приложении или отделении своего банка
- 04** сообщите о звонке/мошенничестве в свой банк (Сбербанк по номеру 900) и в полицию 112

помните, что сотрудники банков и государственных органов не звонят / не пишут в мессенджерах и не отправляют свои личные документы и не заставляют совершать нападения

МОШЕННИКИ ВЗЛАМЫВАЮТ ИЛИ ПОДДЕЛЫВАЮТ АККАУНТ ВАШЕГО ЗНАКОМОГО ЛИБО ВАШ

Какие схемы обмана используют?

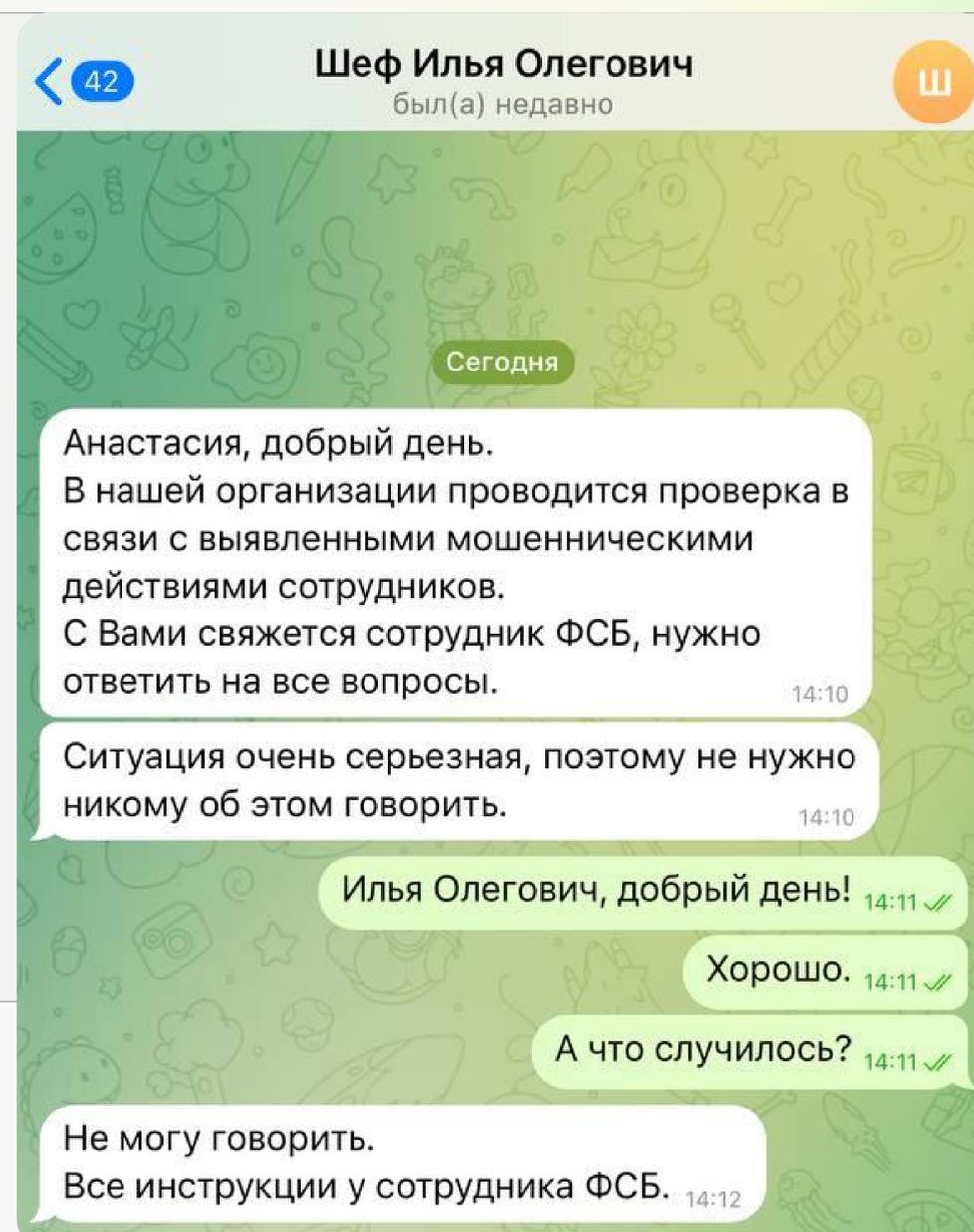


пишут от лица ваших знакомых, друзей, родственников (контактов телефонной книжки) в социальных сетях и мессенджерах:

- от руководителя – **«с вами свяжутся правоохранительные органы»**
- от родственника – **«помоги, переведи денег»**
- от знакомого – **«проголосуй за...»**

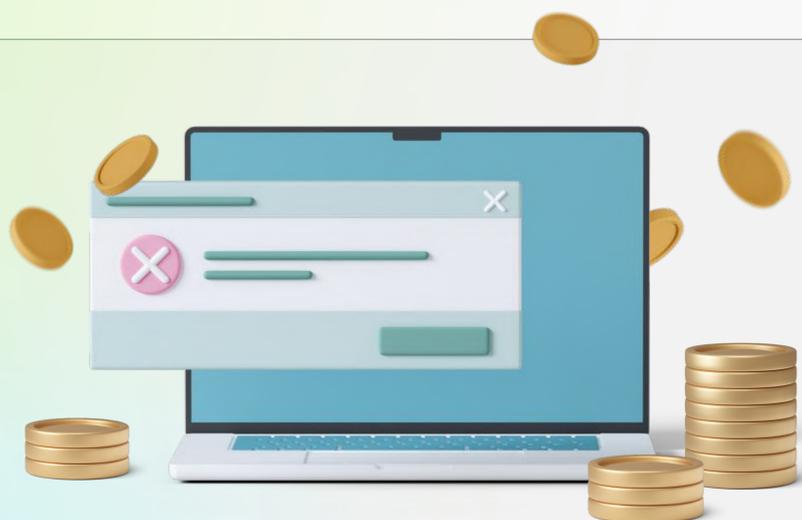
Как защитить себя?

- 01** не переходите по ссылкам / не скачивайте файлы / не устанавливайте программы
- 02** не совершайте никаких переводов, пока не убедитесь, что написал Ваш знакомый
- 03** поменяйте пароли от своих аккаунтов социальных сетей и мессенджеров
- 04** если аккаунт уже взломали - срочно восстановите или заблокируйте его
- 05** сообщите своим родственникам и знакомым о взломе аккаунта



мошенники предлагают быстро заработать / обогатиться

Какие схемы обмана используют?



мошенники пишут в соцсетях и мессенджерах:

- вложите деньги в криптовалюту / финансовые пирамиды
- примите участие в акции, выполните задания для продвижения товаров, услуг
- сотрудничество с «блоггерами», популярными сайтами, компьютерными играми
- получите «выигрыш» или заберите «посылку» оплатив сбор

Как защитить себя?

- 01** не верьте обещаниям быстрого дохода/выигрыша/получения подарков
- 02** не сообщайте свои персональные и банковские данные
- 03** не совершайте покупки / переводы на непроверенных платформах
- 04** не совершайте никаких действий и банковских операций по инструкциям в сообщениях
- 05** сообщите о звонке/мошенничестве в свой банк (Сбербанк по номеру 900) и в полицию 112

