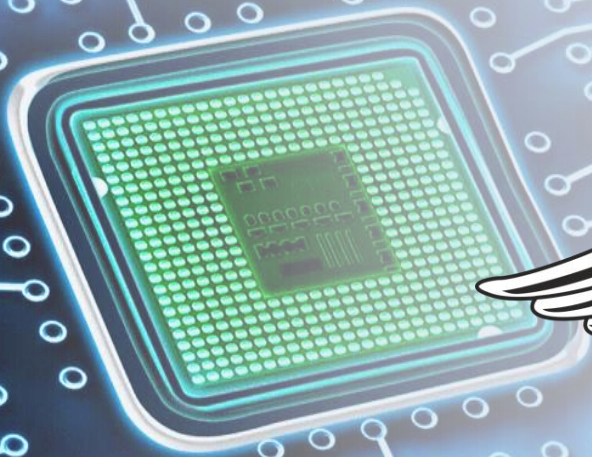


# ПОЛИЦИЯ

## ПРЕДУПРЕЖДАЕТ!





**«Основы  
финансовой  
грамотности –  
защита от  
современных  
преступлений»**

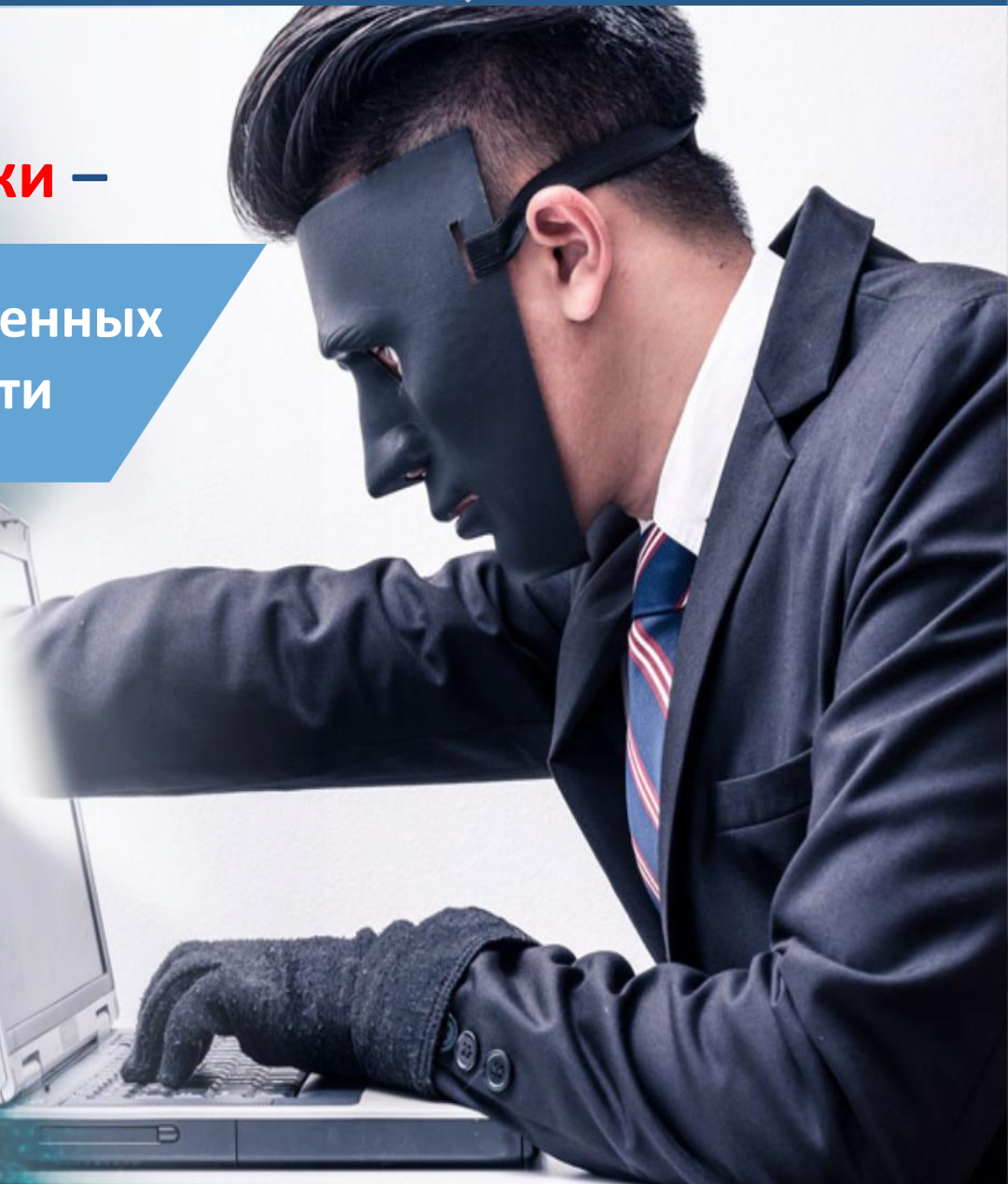






**Дистанционные  
мошенничества и кражи —**

**одни из самых распространенных  
преступлений современности**





Ежедневно в полицию Иркутской области поступает от **3** до **15** сообщений о мошенничестве.

Самая крупная сумма, переведенная аферистам от одного человека –

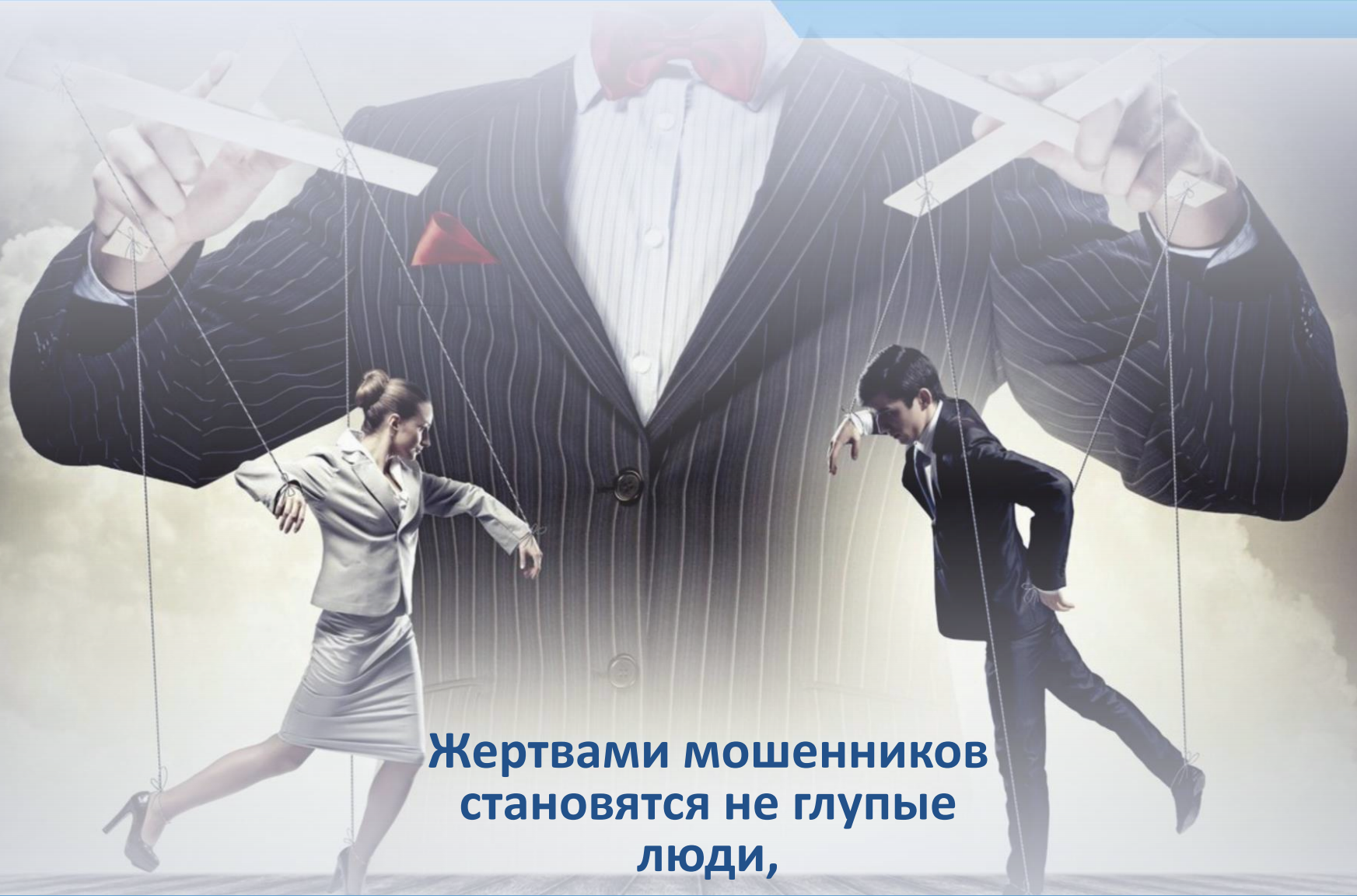
**3,5 млн. рублей.**

Возраст пострадавших от **12** до **90** лет.

Раскрываемость  
мошенничеств

– не более **15%**.





**Жертвами мошенников  
становятся не глупые  
люди,**

**жертвами мошенников становятся люди, подверженные ВЛИЯНИЮ**



**Как  
это  
может  
произойти?**



01

**ЗВОНКИ**



02

**SMS-  
сообщения**



03

**мессенджеры**



04

**почта**



05

**социальные  
сети**



## Способов обмана много, но чаще всего это:



Получение предоплаты либо доступа к счету гражданина при купле-продаже товаров (услуг) в сети Интернет

Смс-сообщения либо звонки от якобы службы безопасности банка



Сообщения либо звонки о происшествиях родственниками, плохих медицинских анализах, компенсациях за различные покупки (услуги), повышение пенсии, дополнительных выплатах, выигрыши в лотерею и пр.





любой мошенник преследует  
**лишь две цели:**  
обманным путем заставить жертву  
перевести денежные средства



Либо создать условия, когда деньги можно  
похитить дистанционно.







## КЕМ ПРЕДСТАВЛЯЮТСЯ МОШЕННИКИ:



специалистом по защите банковских карт от несанкционированного подключения

врачом поликлиники, сообщившим, что вам поставлен тяжелый диагноз и нужно срочно заказать редкое лекарство



сотрудником полиции (адвокатом, прокурором), объясняющим вам, что ваш сын сбил пешехода и за это может угодить в тюрьму или стал участником драки

работником суда или правительства, говорящим о полагающихся компенсациях за ранее приобретенные лекарства, биологические добавки и т.д.



**технически замаскировать любой номер для злоумышленников не составляет большого труда**



# Правило «4x4»

**«4 способа  
идентифицировать  
мошенника  
и**

**4 правила  
не попасться  
на его уловки»**







## Признаки мошенника

Невозможно проверить личность позвонившего

1

Требует действовать здесь и сейчас «ИЛИ БУДЕТ ПОЗДНО!»

2

Просит назвать данные о личности, счете, карте

3

Его предложение сулит выгоду или «защищает» от финансовых потерь

4



## ОСНОВНЫЕ ПРАВИЛА

1

Никому не сообщайте: CVV-коды от банковских карт подтверждающие пароли из СМС

2

Проверяйте информацию в официальных источниках

3

Не переходите по ссылкам от неизвестных отправителей

4

Используйте антивирус





Кем бы ни называл себя человек,  
**которого вы никогда не видели** вживую,  
у нас нет ни единого подтверждения того, что он говорит правду

Проверить это по телефону **НЕВОЗМОЖНО**

**РЕКОМЕНДАЦИЯ:** Прекратите разговор  
и повесьте трубку!



## ВАМ ПРИШЛО СООБЩЕНИЕ:

Поздравляем!  
Вы выиграли  
АВТОМОБИЛЬ!  
Подробности  
по телефону  
X-XXX-XXXXXXX  
Или  
перейдите по  
ссылке  
[https://  
www.....ru](https://www.....ru)

Ваша  
банковская  
карта  
заблокирована!  
Срочно  
свяжитесь по  
номеру  
X-XXX-XXXXXXX  
И сообщите  
свой ПИН КОД

Мама! Я попал  
в беду!  
Срочно  
положи  
деньги на этот  
номер  
X-XXX-XXXXXXX  
Нету связи!  
Потом  
перезвоню!

- \* Проверьте и убедитесь в достоверности информации, которую Вам сообщили в СМС
- \* Не торопитесь выполнять действия, которые от Вас требуют неизвестные.
- \* Не отправляйте СМС на короткие номера, указанные в СМС сообщении
- \* Не открывайте файлы и ссылки, пришедшие в СМС сообщениях с неизвестных номеров



# ПОЛИЦИЯ

НАСТОЯТЕЛЬНО РЕКОМЕНДУЕТ

**СОБЛЮДАТЬ ПРОСТЫЕ  
ПРАВИЛА БЕЗОПАСНОСТИ  
И РАССКАЗАТЬ О НИХ  
ЗНАКОМЫМ И БЛИЗКИМ!**

