Противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Управление МВД России по городу Воронежу

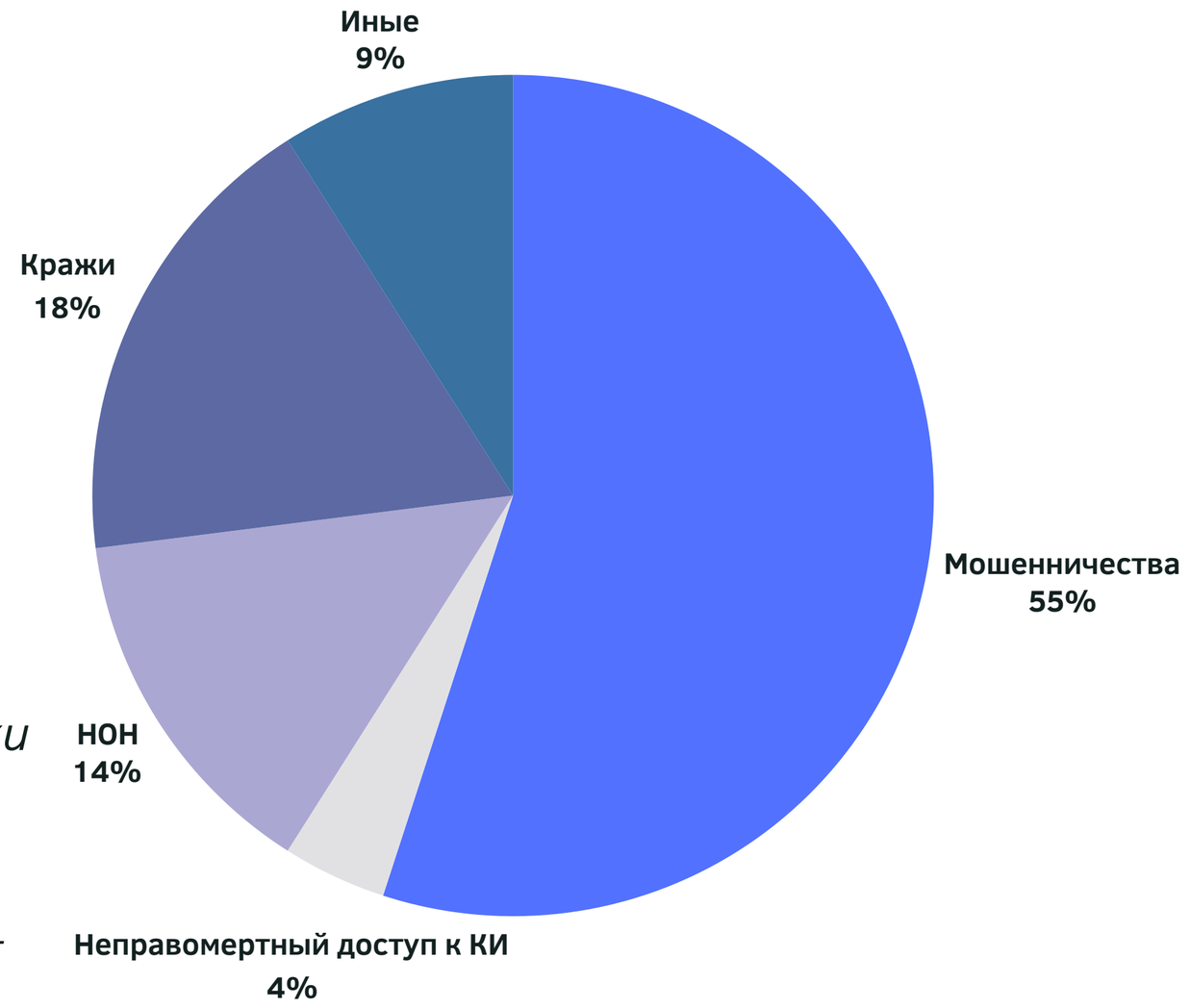
Структура IT - преступлений

За 2024 год

Зарегистрировано 9324 преступления, совершенных с использованием информационно-коммуникационных технологий

Преобладающий вид - преступления против собственности: мошенничества (5100) и кражи (1684)

*Причиненный материальный **ущерб** составил -* ***2 млрд. 474млн. 279 тысяч рублей***



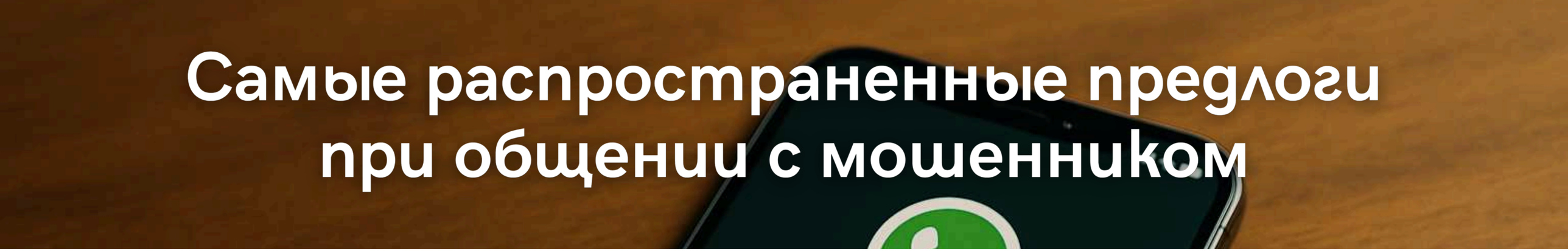
Методы мошенников в 2024 - 2025

- **Социальная инженерия**
- **“Вишинг”** - телефонные мошенничества
- **“Deep Voice” / “Deep Fake Voice” -** использование ИИ при совершении преступлений
- **Фишинг** (“классический”)
- **Вирусы и иное вредоносное ПО**

Социальная инженерия - основа всех схем

Мошенники манипулируют эмоциями: страх, срочность, доверие, чувство вины.

❗ Это не технический взлом, а психологическая атака: человек сам отдаёт данные.



Самые распространенные предлоги при общении с мошенником

Ваш счет в опасности

Для предотвращения попытки завладения вашим аккаунтм с вами свяжется сотрудник Госуслуг, МВД, ФСБ

Продление договора сотовой связи

Требование назвать код из смс для срочного продления договора

Двухэтапное давление

Сначала - явный мошенник. Затем - якобы представитель Росфинмониторинга, МВД, ФСБ, ЦБ и т.д.

“Родственник в беде”

Используя/либо не используя технологии ИИ, звонят и требуют “решить вопрос”, переведя деньги на указанный счет

Расследование по факту финансирования ВСУ

Вас уверяют, что с вашей карты проводится операции по финансированию террористов

Цель мошенников раньше

- Деньги на счетах
- Деньги “под подушкой”
- Ценности, которые можно заложить в ломбард и получить за это деньги

Цель мошенников сейчас

- ВСЕ имеющиеся накопления, сбережения, вклады, драгоценности
- **Кредитные** денежные средства
- **Недвижимость**
- **Автотранспорт**
- **Склонение жертвы к деструктивному поведению** *(акты терроризма, поджоги, диверсии и т.д.)*

Фишинг
(англ. phishing от fishing «рыбная ловля, выуживание»)

Мошенники используют поддельные интернет-ресурсы, визуально неотличимые от официальных сайтов банков, маркетплейсов и других популярных сервисов. Человек вводит данные своей банковской карты (номер, срок действия, CVV-код), не подозревая, что ресурс принадлежит злоумышленникам. В результате происходит несанкционированный доступ к средствам.

📌 Основные признаки фишингового сайта:
- доменное имя отличается на 1-2 символа;
- навязчивые уведомления о "выгодных акциях";
- просьба срочно ввести платёжные данные.

Внимательно проверяйте реквизиты Интернет-ресурса и не переходите по ссылкам от незнакомцев

Предложения быстрого обогащения

Сомнительные схемы:

1. *“Дай карту”*
2. *“Просто прими перевод и отправь куда скажу”*
3. *Работа курьером: “забери у бабушки деньги и отправь куда скажу”*
4. *“Закажи на себя посылку, всё будет нормально”*

Инвестиции или быстрый заработок

Спойлер: можно серьезно “вляпаться”

Трейдинг

Предлагают вложиться в криптобота, который торгует только в плюс или в биржу под присмотром персонального наставника

Инвестиции в криптовалюту

Предлагают стать ранним участником проекта с огромными девидендами.

В результате таких инвестиий Вы можете быть вовлечены в схему **“криптовалютного треугольника”**, где мошенник, манипулируя Вами, перечисляет похищенные деньги между счетами третьих лиц

Взлом “Госуслуг”

Получение доступа к учетной записи порталал *“Госуслуги”* - излюбленная “тема” мошенников

- **Вирусы**
- **Иное вредоносное ПО**
- **Восстановление доступа к старому абонентскому номеру**
- **Социальная инженерия**

Сомнительный звонок?

Не называй код из СМС!

Звонят заменить счетчики, при этом требуя код из СМС?

Звонят записать Вас в "новую очередь" в поликлинике, при этом требуя код из СМС?

Звонят потому что у Вас заканчивается срок договора сотовой связи, при этом требуя код из СМС?

ЭТО - МОШЕННИКИ!
ПРЕРВИ РАЗГОВОР

Основные советы по финансовой и цифровой безопасности

- Никогда и никому не называть коды из СМС
- Помнить: безопасных счетов не существует
- Не отвечать на звонки в мессенджерах с незнакомых номеров
- Критически относиться ко всем звонкам и просьбам во время телефонного разговора. Недопустимо **вслепую** доверять собеседникам из “официальных” и “государственных” учреждений.
- Переход по подозрительным ссылкам может привести к хищению ваших персональных данных и платежной информации