Прокуратура г. Воркуты

КИБЕРМОШЕННИКИ: как распознать и не потерять свои сбережения



г. Воркута, 2026 год

Ежедневно в России регистрируются тысячи преступлений с использованием IT-технологий. Злоумышленники постоянно придумывают новые способы обмана, похищая у граждан миллиарды рублей. Чтобы защитить себя, важно знать основные схемы и уметь вовремя распознать угрозу.

Какие схемы используют мошенники сегодня?

1. Звонки от «сотрудников банка» или «полиции».

Вам звонят и сообщают о подозрительной операции, попытке взлома счёта или оформлении кредита. Для «спасения» просят назвать код из SMS, перевести деньги на «безопасный счёт» или установить приложение для удалённого доступа. Запомните: настоящий банк никогда не просит коды и не требует переводить деньги!

2. Фишинговые сайты и поддельные приложения.

Вы получаете SMS или e-mail со ссылкой, где предлагают подтвердить данные карты, оплатить налог за выигрыш или обновить приложение банка. Сайт выглядит как настоящий, но все введённые данные уходят мошенникам. Всегда проверяйте адресную строку и скачивайте приложения только из официальных магазинов.

3. Лжеинвестиции и «быстрые деньги».

В соцсетях или мессенджерах предлагают сверхдоходные вложения в криптовалюту, акции или «уникальный стартап». Сначала вы получаете небольшую прибыль, затем Вас уговаривают вложить крупную сумму — после чего брокер исчезает. Помните: гарантированного высокого дохода не бывает.

4. Взлом аккаунтов в соцсетях и мессенджерах.

Злоумышленники взламывают страницу вашего друга или родственника и от его имени просят срочно перевести деньги «на лечение», «на операцию» или «в долг». Всегда перезванивайте человеку и уточняйте лично.

5. Мошенничество с «Госуслугами»

Приходит сообщение о необходимости подтвердить учётную запись, иначе доступ заблокируют. Для этого просят назвать код подтверждения из SMS. Получив доступ к вашему профилю, мошенники могут оформить кредиты или запросить ваши персональные данные.

6. Поддельные сайты знакомств и объявлений

Под видом покупателя или продавца Вас просят перейти по ссылке для оплаты или получения предоплаты. Ссылка ведёт на фишинговую страницу. Никогда не переходите по подозрительным ссылкам и не сообщайте код из SMS.



Что нового в законодательстве для защиты граждан?

С 1 марта 2025 года вступил в силу закон о самозапрете на кредиты (Федеральный закон от 26.02.2024 № 31-ФЗ). Теперь каждый гражданин может бесплатно установить в своей кредитной истории запрет на заключение договоров потребительского займа без личного присутствия. Это надёжно защищает от мошенников, которые пытаются оформить кредит по украденным паспортным данным.

Кроме того, с 1 июня 2025 года ужесточены правила использования сим-карт: запрещено передавать SIM-карты третьим лицам, а операторы обязаны блокировать номера, с которых совершаются подозрительные звонки. Это снижает количество анонимных обзвонов.

Как защитить себя: простые правила

· Не доверяйте звонкам из «банка» — кладите трубку и перезванивайте по официальному номеру, указанному на карте.

· Никогда не сообщайте коды из SMS, пароли, CVV-код, данные паспорта по телефону или в интернете.

· Проверяйте адрес сайта — даже одна лишняя буква в имени может выдать мошеннический ресурс.

· Установите самозапрет на кредиты через «Госуслуги» или МФЦ — это бесплатно и надёжно.

· Не переходите по ссылкам из подозрительных сообщений, даже если они пришли от друзей (их аккаунт могли взломать).

· Используйте сложные пароли и включите двухфакторную аутентификацию везде, где это возможно.

· Регулярно проверяйте выписки по картам и кредитную историю — это поможет вовремя заметить несанкционированные действия.



Что делать, если вы столкнулись с мошенничеством?

1. Немедленно заблокируйте карту через мобильное приложение или горячую линию банка.

2. Сохраните все доказательства — скриншоты, переписки, номера звонящих.

3. Напишите заявление в полицию (можно через сайт МВД или по телефону 102).

4. Обратитесь в банк с заявлением о возврате денег (в течение 30 дней с момента операции у вас есть шанс оспорить перевод).

5. Установите самозапрет на кредиты, если ещё не сделали этого.



Помните: ваша финансовая грамотность и бдительность — главная защита от мошенников. Не стесняйтесь прерывать подозрительные разговоры и перепроверять информацию. Лучше потратить пять минут на проверку, чем потерять все накопления.

В случае любых сомнений или подозрительных предложений:

- НЕМЕДЛЕННО прекращайте общение.
- Позвоните на горячую линию вашего банка.
- Сообщите о попытке мошенничества в правоохранительные органы (например, через официальный сайт МВД России или по телефону 102).

Прокуратура г. Воркуты
169900, г. Воркута, ул. Яновского, д. 1.