Распространенные схемы мошенничества, совершаемые на территории города Перми в 2024-2025 годы

1. Мошенничества с использованием AI (голосовой клонинг, deepfake).
Суть: Злоумышленники используют нейросети для имитации голоса близких (звонок «от ребенка» с просьбой о срочном переводе денег) или создают поддельные видео в реальном времени.
Защита: Всегда перезванивайте на известные Вам номера, чтобы подтвердить личность. Установите кодовое слово в семье.

2. Фишинг через «Официальные» организации.
Суть: Поддельные SMS/письма от банков, госорганов (налоговая, Роспотребнадзор), курьерских служб со ссылками на фейковые сайты для кражи данных.
Пример: «Ваша карта заблокирована», «Неуплаченный штраф», «Посылку нельзя доставить».
Защита: Не переходите по ссылкам. Звоните в организацию по официальному номеру сайта.

3. Мошенничество на маркетплейсах (Avito, Юда и др.)
Суть: Предоплата за товар с последующим исчезновением продавца; фейковые страницы «поддержки»; фиктивные арендодатели.
Защита: Платите только при получении или через безопасные способы оплаты маркетплейса.

4. Схемы с инвестициями и «быстрым заработком».
Суть: Фейковые брокеры, криптопекты с гарантированной доходностью, финансовые пирамиды под видом «новых технологий».
Защита: Проверяйте лицензии ЦБ РФ. Помните: высокая доходность = высокий риск.

5. Звонки от «сотрудников банка/полиции».
Суть: Мошенник представляется сотрудником безопасности банка («несанкционированный перевод») или полицейским («родственник в беде, нужны деньги»), чтобы заставить перевести деньги на «безопасный счет».
Защита: Банки и полиция никогда не просят переводить деньги на другие счета. Положите трубку и перезвоните в организацию.

6. Техническая поддержка (Tech-support-scam).
Суть: Всплывающие окна в браузере или звонки с предупреждением о «вирусе». Мошенники получают доступ к устройству или вымогают деньги.
Защита: Никогда не предоставляйте удаленный доступ к компьютеру незнакомцам.

7. Мошенничество в соцсетях и на сайтах знакомств (Romance scam).
Суть: Долгое общение с созданием доверительных отношений, после чего следует просьба о денежной помощи («билеты», «лечение»).
Защита: Будьте скептичны к онлайн-знакомствам, никогда не отправляйте деньги людям, которых не видели в живую.

8. Скимминг и кража данных карт.
Суть: Установка устройств на банкоматы для считывания данных, а также фишинговые сайты для кражи CVV-кода.
Защита: Закрывайте рукой клавиатуру при вводе PIN, используйте бесконтактную оплату (NFC) или карты с дополнительной защитой.

9. Мошенничество со льготой и субсидиями.
Суть: Предложения оформить «неиспользованные льготы», «социальные выплаты» за комиссию.
Защита: Все льготы оформляются только через госорганы (МФЦ, портал Госуслуг) бесплатно.

10. Взлом мессенджеров и соцсетей.
Суть: Взлом аккаунта и рассылка сообщений друзьям с просьбой одолжить деньги («срочно, сам не могу зайти»).
Защита: включите двухфакторную аутентификацию.

Общие правила безопасности:
1. Никому не сообщайте коды из SMS, CVV-код карты, пароли.
2. Не торопитесь действовать под давлением («срочно!», «иначе счет заблокируют!»).
3. Проверяйте информацию через официальные источники.
4. Установите антивирус и обновление ПО.

Если столкнулись с мошенничеством:

- немедленно позвоните в банк для блокировки карты;
- обратитесь в полицию (можно через сайт МВД или Госуслуги) или в ближайшее отделение полиции.

Управление МВД России по городу Перми