**Депбезопасности Югры информирует:**

В 2024 году в Югре зарегистрировано 7,6 тысяч дистанционных краж и мошенничеств, общий ущерб от которых превысил 3,055 млрд рублей, что более чем в 2 раза превышает показатель 2023 года и в 4,3 раза показатель 2022 года.

В среднем за одни сутки в автономном округе совершается
20 преступлений, ущерб от которых составляет более 8 млн рублей.

В ноябре 2024 года были зафиксированы «антирекорды» – два жителя Нижневартовска и Сургута передали мошенникам 35 и 49 млн рублей соответственно.

Самыми распространенными способами дистанционных мошенничеств остаются:

телефонные звонки от псевдо-сотрудников различных ведомств и организаций;

сделки купли/продажи на сайтах;

«инвестирование» (покупка криптовалюты, ценных бумаг и т.д.).

Опрос потерпевших показывает, что 99% из них знали о потенциальной угрозе и основных схемах мошенничеств.

Жертвами мошенников становятся все категории граждан независимо от возраста, образования, социального статуса и имущественного положения.

Мошенники совершенствуют методы и схемы обмана граждан, в том числе используют технологии социальной инженерии.

Преступники предварительно собирают сведения о человеке, в том числе в социальных сетях. В последующем используют данные сведения, чтобы втереться в доверие к потенциальной жертве и ею манипулировать, вплоть до склонения к противоправному поведению (участие в диверсиях, поджогах и т.д.).

Рекомендуем следовать простым правилами и психологическим установкам:

* **никому не доверять без проверки информации (принцип нулевого доверия);**
* **перед принятием решения поставить ситуацию «на паузу» для проверки информации;**
* **доверять своим сомнениям;**
* **не позволять собой манипулировать, если речь идет об использовании или передаче персональных данных; «сохранении» или «преумножении» финансовых средств.**

Предлагаем **прекращать дистанционное общение** (по телефону, в мессенджерах, социальных сетях), если разговор с незнакомым собеседником переходит к необходимости передачи персональных данных, сохранению, преумножению или передаче денежных средств, угрозам привлечения к ответственности за невыполнение требований.

При это необходимо учитывать, что с развитием IT-технологий прогнозируется увеличение фактов мошенничества с применением дипфейков (технологический синтез изображения или голоса иного лица).

# Управлением по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России информация о применяемых новых схемах мошенничества и способах им противодействия размещается в телеграмм-канале **«Вестник Киберполиции России**»: [https://t.me/cyberpolice\_rus.](https://t.me/cyberpolice_rus)