**Памятка, которая поможет избежать обмана:**

1. Не спешите. Вам предлагают сделать немедленно? Подождите пару дней, вполне возможно, что через пару дней интернет-ресурс, на который вас вела ссылка, уже не будет существовать.

2. Не вводите конфиденциальные данные на неизвестных компьютерах или компьютере без антивирусного программного обеспечения.

3. Будьте бдительны. Никогда не доверяйте даже знакомым людям в сети. Может оказаться, что с вами общаются злоумышленники, а не ваши знакомые.



4. Не доверяйте малознакомым лицам, которые пытаются связаться с вами от имени каких-либо финансовых, государственных и т.п. организаций с целью уточнения конфиденциальных данных.

5. Проверяйте по телефонам служб поддержки любые обращения и просьбы, полученные через интернет и связанные с конфиденциальными данными или финансами.

6. Любые финансовые вопросы обговаривайте при личной встрече, если это возможно.

7. Не переводите деньги на малозащищённые сервисы типа «ЯндексДеньги», работа которых не предполагает глубокой идентификации пользователей (кто в действительности получил ваши деньги, никто никогда не узнает).

8. Принцип «не уверен - не делай!». Если дизайн ранее знакомого вам сайта, его работа, адрес в строке браузера или размещённая реклама отличны от привычного вам вида, ни в коем случае не вводите конфиденциальные данные.

9. Для совершения покупок в сети Интернет заведите отдельную карту с минимальным количеством денежных средств.

10. Установите запрет отправки сообщений на короткие номера. Данная услуга доступна у всех операторов.

**Если вы всё же стали жертвой мошенников, сделайте всё возможное, чтобы исключить возможность дальнейшего причинения вам ущерба. Свяжитесь с оператором и отпишитесь от платных сервисов.**

**Прокуратура Красноярского**

**Астраханской**

**области**

**РАЗЪЯСНЯЕТ:**

# «Дистанционное мошенничество или правила сетевой безопасности»



**с. Красный Яр**

**2024 год**