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.

Ленинградская межрайонная природоохранная прокуратура

РАЗЪЯСНЯЕТ:

«Дистанционное мошенничество, или правила сетевой безопасности»

С развитием современных цифровых технологий появился новый тип мошенничества - дистанционный. Мобильная связь, электронная почта, социальные сети, интернет-банкинг, интернет-торговля и другие цифровые сервисы и технологии дают мошенникам огромные возможности для обмана доверчивых и отзывчивых россиян.

Уголовный кодекс РФ в статье 159 определяет мошенничество как хищение чужого имущества или приобретение права на чужое имущества путем обмана или злоупотребления доверием. Наказание - вплоть до лишения свободы на срок до двух лет и более, однако это не останавливает злоумышленников. Рассмотрим наиболее частые методы обмана, от которых страдают простые доверчивые люди в сети Интернет и в которых основным слабым звеном становится именно сама жертва.

Фишинг - дословно можно перевести как **«выуживание»**. Мошенники с помощью e-mail спама или рекламы на не безопасных интернет-ресурсах заманивают жертву на интернет-страницы, не отличимые по внешнему виду от оригинальных сайтов банков, интернет-магазинов, платёжных систем, социальных сетей и других сервисов, требующих авторизации. Применяя различные психологические методы мотивации, злоумышленники подталкивают жертву самостоятельно ввести свои данные в формы поддельных сайтов.

Мобильные сервисы и SMS – чаще всего используются для отправки сообщений с просьбой о переводе денег на счёт злоумышленника. SMS составляется в такой форме, чтобы на неё среагировало как можно больше потенциальных жертв. Например, «Мама, срочно положи 100 рублей на мой номер 8.....104, завтра верну!».

Часто злоумышленники представляются оператором связи и рассылают «запросы» с длинной USSD-командой, предназначенной для перевода денег на номер злоумышленника.

Еще один вариант — вам приходит SMS с обычного номера о зачислении на ваш счет средств, а после следует ещё одно сообщение с просьбой вернуть «зачисленные по ошибке» деньги на какой-либо номер.

Нередки случаи, когда мошенники рассылают сообщения о блокировке карты или снятии средств от имени банка. Помните, что настоящие SMS-подтверждения приходят с короткого сервисного номера оператора, но никак не с обычного «+7....».

Существует также весьма действенная мошенническая схема развода на деньги с помощью SMS: сайты просят указать для доступа к тому или иному платному контенту ваш номер сотового телефона. После этого с вашего счета ежедневно списывается определённая сумма и происходит это почти легально — указав свой номер, вы автоматически «оформили» подписку на платный сервис.

Также нередко злоумышленники напрямую звонят жертве и под различными предлогами пытаются узнать данные, например, кредитной карты, или представляются родственниками, попавшими в беду, и просят денег.