

Памятка для граждан об основных способах мошенничества.

Некоторые способы телефонного мошенничества и меры защиты:

- Звонки от «банков», «полиции» или «службы безопасности» с просьбой сообщить данные карты, пароли или перевести деньги. Настоящие сотрудники банков или государственных органов никогда не запрашивают такую информацию по телефону;
- Поддельные SMS с ссылками на фальшивые сайты (фишинг);
- «Ваш родственник в беде» — просьба срочно отправить деньги;
- Подмена номеров - мошенники часто используют технологии подмены номера, чтобы их звонок выглядел как звонок из банка или государственного учреждения. Не доверять номеру, который отображается на экране, если есть сомнения, всегда перезванивать по официальному номеру.

Проверить информацию по официальным каналам — если звонят из «банка» или «правоохранительных органов» и сообщают о подозрительных операциях, немедленно прервать разговор. Самостоятельно позвонить в службу поддержки банка по номеру, указанному на банковской карте (обычно на обратной стороне), или на официальном сайте банка.

Не переходить по ссылкам в сообщениях и не скачивать файлы - мошенники могут прислать сообщения в мессенджерах или SMS после разговора и попросить открыть их.

Некоторые способы мошенничества в интернете и меры защиты:

- Фишинг - мошенники создают поддельные сайты и письма, похожие на настоящие, чтобы получить конфиденциальные данные пользователей;
- Мошенничество с рассылками предложений и «подработке» - мошенники рассылают привлекательные сообщения о лёгких деньгах или высокооплачиваемой работе без усилий, пытаясь получить паспортные данные, информацию о банковских картах;
- Взломанные аккаунты друзей и знакомых - мошенники взламывают аккаунты знакомых или создают их копии, чтобы писать сообщения о срочной финансовой помощи («попал в беду», «сломался телефон»,

«банк не работает»). Если сообщение кажется странным, связаться с другим способом (по телефону или лично) и уточнить, писал ли он вам;

- Фальшивая реклама в социальных сетях - мошенники размещают рекламу с обещанием огромных скидок и эксклюзивных товаров в соцсетях, на сайтах или через рассылки. После перехода по ссылке пользователь попадет на поддельный сайт магазина, внешне похожий на настоящий;
- Финансовые пирамиды - мошеннические схемы, где обещают доход от «инвестиций». Сначала могут выплачивать реальные деньги для создания доверия, но на деле прибыль формируется только за счёт привлечения новых участников;

Некоторые способы мошенничества при личных встречах и меры защиты:

- Обман «магов» и «гадалок» — они предлагают снять порчу за деньги;
- Псевдо-благотворительные сборы;
- Продажа несуществующих товаров или услуг;

Не доверять незнакомцам, например, если к дому пришли незнакомцы, не стоит им доверять, сначала нужно попросить, чтобы они предоставили документ, доказывающий, что они работают на том или ином предприятии.

Не передавать незнакомцам деньги - они могут понадобиться злоумышленникам для снятия порчи, обмена крупных купюр и так далее.

Если человек столкнулся с мошенниками, необходимо немедленно позвонить в банк, чтобы заблокировать карту, обратиться в полицию по номеру 102 или через официальный сайт МВД, сообщить о мошенничестве в Роскомнадзор или на «Госуслугах».