**1. Мошенничество по телефону**

Мошенники могут звонить под видом сотрудников банков, полиции, социальных служб или других официальных организаций.

**Как работает схема:**

* Злоумышленники сообщают, что ваша банковская карта или счет подверглись атаке, и просят вас передать личные данные, одноразовые пароли или выполнить перевод средств.
* Сообщают, что на ваше имя взяли кредит, и предлагают "помощь" в его отмене.
* Информируют вас о том, что вы являетесь свидетелем по уголовному делу и необходимо прибыть в город Москву на допрос. На ваш отказ предлагают «урегулировать» вопрос дистанционно, передав свои личные данные.

**Что делать:**

* Не передавайте личные данные и пароли по телефону.
* Завершите разговор и перезвоните в банк по официальному номеру.
* Никогда не совершайте переводы по инструкциям незнакомцев.
* Не скачивать и не устанавливать на свой телефон (или компьютер) программы.

**2. Фишинговые сайты и сообщения**

Фишинг - это попытка получить вашу личную информацию (пароли, данные карты) через поддельные сайты или сообщения, которые выглядят как настоящие.

**Как работает схема:**

* Вы получаете письмо или сообщение с ссылкой на поддельный сайт, где просят ввести данные вашей банковской карты или пароли.
* Часто такие сайты визуально неотличимы от оригинальных, но адрес сайта может быть слегка изменен.

**Что делать:**

* Не переходите по ссылкам из подозрительных сообщений и писем.
* Всегда проверяйте адрес сайта, прежде чем вводить данные.
* Используйте антивирусные программы, которые могут выявлять поддельные сайты.

**3. Мошенничество через мессенджеры и социальные сети**

Мошенники могут обращаться к вам через мессенджеры или социальные сети, притворяясь вашими друзьями, коллегами или представителями компаний.

**Как работает схема:**

* Мошенники пишут, что ваш знакомый в беде и срочно нуждается в деньгах.
* Просят сообщить номер карты или перевести средства для выигрыша, участия в акции или возврата средств.

**Что делать:**

* Всегда проверяйте информацию, связавшись с человеком напрямую по телефону.
* Не переводите деньги по просьбам через мессенджеры.
* Помните, что официальные организации не будут обращаться через личные аккаунты в социальных сетях.

**4. Мошенничество через объявления на сайтах купли-продажи**

На сайтах объявлений мошенники часто выдают себя за покупателей или продавцов товаров и услуг.

**Как работает схема:**

* При продаже товара мошенник заявляет, что готов перевести деньги, но просит вас перейти по ссылке для "получения" средств, где нужно ввести данные карты — это фишинговый сайт.
* При покупке товара мошенник может потребовать предоплату за товар или услугу, но после получения денег перестает выходить на связь и не отправляет товар.

**Что делать:**

* Никогда не переходите по подозрительным ссылкам, особенно если вам предлагают "получить деньги".
* Используйте безопасные методы оплаты, такие как безопасные сделки на платформах объявлений.
* Проверяйте информацию о продавце, читайте отзывы, не соглашайтесь на полную предоплату.

**5. Мошенничество с выигрышами и лотереями**

Мошенники часто используют фальшивые уведомления о выигрыше в лотереях или конкурсах, в которых вы не участвовали.

**Как работает схема:**

* Вы получаете сообщение или звонок с информацией о том, что стали победителем розыгрыша, лотереи или получили крупный приз.
* Для получения "выигрыша" вас просят оплатить комиссию, налоги или другие сборы, либо предоставить личные данные (паспорт, банковскую карту).

**Что делать:**

* Если вы не участвовали в розыгрыше, будьте уверены, что это мошенничество.
* Никогда не переводите деньги и не предоставляйте данные карты в обмен на обещание получения приза.
* Проверяйте информацию о конкурсах на официальных сайтах, а также читайте условия розыгрышей.

**6. Мошенничество с технической поддержкой**

Мошенники могут притворяться сотрудниками служб технической поддержки (например, интернет-провайдеров, мобильных операторов или даже крупных ИТ-компаний).

**Как работает схема:**

* Мошенники звонят или отправляют сообщение, представляясь сотрудниками службы технической поддержки (например, интернет-провайдера или компании-разработчика программного обеспечения), и сообщают, что на вашем устройстве обнаружена проблема или вирус.
* Для "решения проблемы" они просят установить специальное программное обеспечение, которое на самом деле является вредоносным, или предоставить удаленный доступ к вашему устройству.
* После этого они могут получить доступ к личным данным, паролям и финансам, или требовать деньги за "устранение" несуществующей угрозы.

**Что делать:**

* Никогда не устанавливайте ПО или не передавайте доступ к устройству по запросам неизвестных.
* Если вам позвонили под видом технической поддержки, завершите звонок и обратитесь в официальную службу поддержки через проверенные контакты.
* Обновляйте антивирусное ПО и системы безопасности на ваших устройствах.

**Основные рекомендации по защите от дистанционного мошенничества:**

1. **Никогда не передавайте личные данные, пароли и банковские реквизиты по телефону, в интернете или через SMS.**
2. **Будьте бдительны к подозрительным предложениям, особенно если они связаны с деньгами или личной информацией.**
3. **Проверяйте достоверность сайтов, сервисов и организаций через официальные источники.**
4. **Используйте двухфакторную аутентификацию для защиты своих онлайн-аккаунтов.**
5. **Всегда перезванивайте в банк или организацию по официальным номерам в случае подозрительных звонков.**