Дистанционные мошенничества становятся все более изощренными, и важно быть осведомленным о том, какие распространенные схемы используют злоумышленники. Это поможет не стать жертвой преступления и защитить свои средства и данные.

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.

7. Мошенничество с использованием социальных сетей

Сообщение от руководителя

Как работает схема:

Злоумышленники, доподлинно зная о том, что их жертва трудоустроена в какой-либо организации, создают клон страницы в социальной сети (Вконтакте, Telegram, Whatsapp) руководителя данной организации, после чего от его лица сообщают гражданину о якобы проводимой в их организации проверки ФСБ России факта перечисления сотрудниками организации денежных средств в поддержку Вооруженных Сил Украины.

После сообщения данного факта жертве непременно звонят якобы сотрудники ФСБ России и сообщают, что с их банковских счетов осуществляются переводы денежных средств на нужды Вооруженных Сил Украины.

Патриотически-настроенные граждане, думая о том, что их деньги могут оказаться в руках противника, выполняют все указания мошенников.

Что делать:

Для того, чтобы не стать жертвой такой схемы мошенничества, следует:

* немедленно прекратить телефонный разговор;

* уведомить руководителя о получении указаний от его лица через социальную сеть, предупредить других сотрудников об этой ситуации;

* при необходимости через приложение банка заблокировать доступ к своим банковским счетам;

* обратиться в органы полиции.

Мошенничество с использованием сообщений о фото в Интернете

Как работает схема:

Гражданину в социальной сети или интернет-мессенджере (ВКонтакте, Telegram, WhatsUp) приходит сообщение от клона профиля знакомого ему лица с текстовым сообщением «Это твои фотографии?/Это ты на видео?/Ты знаешь этого человека?» с приложением ссылки или стороннего файла любого другого формата.

Текст сообщения может варьироваться. В любом случае содержание такого сообщения направлено на побуждении интереса у лица к открытию и прочтению сообщения.

При последующем открытии приложенной ссылки или стороннего файла происходит автоматическое скачивание вредоносного приложения, которое предоставляет мошенникам полный дистанционный доступ к мобильному устройству гражданина, что и позволяет в последующем осуществить хищение принадлежащих ему денежных средств.

Что делать:

Чтобы обезопасить себя от такого типа мошенничества следует помнить, что открывать диалоговое окно с приложенным файлом или ссылкой безопасно, но в последующем следует:

* детально изучить полученное сообщение: установить, является ли профиль отправителя «подлинным»,

* проверить контактны данные, обратить внимание на отсутствие в диалоге иных сообщений и медиа-файлов;

* обратить внимание на текст ссылки и формат приложенного файла. Следует остерегаться форматов «exe». Зачастую мошенники прикладывают файл с наименованием «mamont».

В случае открытия вредоносного файла мобильное устройство начнет производить самостоятельные бесконтрольные действия. Попробуйте незамедлительно выключить его длинным нажатием клавиши «блокировка» или физическим извлечением батареи.

Если мошенникам все же удалось похитить денежные средства незамедлительно обращайтесь в полицию. Ни в коем случае не форматируйте мобильное устройство, оставшиеся на нем сведения важны для осуществления расследования.

8. Мошенничество с использованием популярных детских онлайн игр

Как работает схема:

Все большую популярность приобретает мошенничество в популярных среди детей онлайн играх, примером служит игра Roblox (роблокс).

В ходе игры детям предлагается подписаться на страницу в социальной сети Телеграмм, где разыгрывается пополнение игрового счета. Для перечисления выигрыша, злоумышленники просят ребенка сфотографировать банковское приложение в телефоне родителей (сфотографировать банковскую карту, осуществить перевод денежных средств через приложение банка и пр.), требуют это сделать незамедлительно, объясняя тем, что приз скоро исчезнет.

После того, как ребенок выполнит указания, денежные средства со счета родителей уходят к мошенникам.

В основном в такую ситуацию попадают дети в возрасте Самый «удобный» от 7 до 12 лет. Дети этого возраста уже разбираются в компьютерной технике, смартфонах и

соцсетях. Если в семье не выстроен доверительный диалог, велика вероятность, что ребенок без спроса возьмет телефон/банковскую карту родителей чтобы получить как можно скорее заветный приз.

Что делать:

Родителям важно защитить детей от мошенников. Необходимо:

* проверять приложения, которые использует ребенок,

*разговаривать с ним об угрозах в сети и правилах безопасного поведения в интернете;

* необходимо объяснить ребенку, что вводить данные банковских карт или делиться иной личной информацией в интернете нельзя.

Основные рекомендации по защите от дистанционного мошенничества:

- 2□ **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.**
- 2□ **Проверяйте достоверность сайтов, сервисов и организаций через официальные источники.**
- 2□ **Используйте двухфакторную аутентификацию для защиты своих онлайн-аккаунтов.**
- 2□ **Всегда перезванивайте в банк или организацию по официальным номерам в случае подозрительных звонков.**