Информация
для граждан о профилактике и предупреждении дистанционных преступлений в сфере
информационно-телекоммуникационных технологий:

Самые распространенные схемы мошеннических действий в сфере информационно-телекоммуникационных технологий;

1. **Звонки и сообщения от «работников» банка.** (Обычно мошенники звонят клиентам от имени службы безопасности банка и сообщают о том, что на их счёте обнаружена подозрительная активность. Иногда они утверждают, что со счёта пытались перевести крупную сумму или взять на ваше имя кредит).

2. **Смс-рассылки или электронные письма е сообщениями о выигрыше.** (Одна из популярных схем, которые часто используют мошенники в интернете. Обычно это происходит так: на сайте вы видите баннер, на котором написано: «Вы выиграли **100.000** рублей!». Для того чтобы получить выигрыш, вам предлагается перейти по ссылке. Там вы видите, что для получения денег необходимо оплатить взнос. Он может быть представлен как налог на выигрыш или комиссия лотереи).

3. **Фишинговые сайты.** (Если вы являетесь продавцом какой-либо вещи, то обычно мошенник присылает вам сообщение о том, что покупка уже оплачена и просит для получения денег перейти по ссылке на сайт, который похож на реальный сервис. Чаще всего такие сайты оформлены в стилистике известных банков).

4. **Обман при оказании фриланс-услуг.** (В современном мире многие специалисты стремятся перейти на удалённую работу. В процессе поисков можно часто встретить объявления, которые обещают простой и быстрый заработок. Но, когда вы начинаете общаться с работодателем, выясняется, что для начала работы нужно внести плату за доступ к заказам или обучающие материалы.

5. **Мошенничество в онлайн-играх.** (Не только дети, но и взрослые люди любят играть в компьютерные игры. Такое виртуальное развлечение обычно требует улучшения своих персонажей, которое требуется приобретать за реальные деньги. Многие люди пытаются сэкономить и найти того, кто продаст предметы для повышения уровня подешевле. Здесь также можно наткнуться на мошеников, которые заберут предоплату за продукт и ничего не предоставят взамен).

6. «Крик о помощи» (Мошенники отличные психологи, они давят на эмоции жертв, например, желание помочь, чтобы поймать тех на крючок. В интернете появляется душераздирающая история о борьбе маленького человека за жизнь. Время идёт на часы. Срочно необходимы дорогие лекарства, операция за границей и т.д. Просят оказать помощь всех неравнодушных и перевести деньги на свои реквизиты).

7. **СМС по поводу объявления.** (Этим способом чаще всего пользуются аферисты, работающие посредством сервисов бесплатных объявлений, например, Avito или Юла. Они пишут продавцу SMS с вопросами о товаре и предлагают для дальнейшего общения перейти по ссылке. Если вы сделаете это, то, возможно будете перенаправлены на подставной сайт, при оплате на котором с вашего счета будут списаны деньги. Существует еще один вариант мошенничества по этой схеме, при котором продавец попросит внести предоплату за бронирование товара и после этого не выходит на связь).

8. **Приложения для смартфонов.** (Под видом обычных программ, которые вы желаете установить на своё устройство, могут скрываться зловредные приложения, несущие в себе вирус или открывающие доступ к личным данным. Кибермошенники активно этим пользуются. Загружайте приложения только через официальные магазины Google Play, App Store, Rustore и т.д.).

9. **Использование личных сведений** (персональных данных) из социальных сетей в противоправных целях. Например, чтобы войти в доверие человека при реализации вышеуказанных схем мошенничества.

Чтобы не оказаться жертвой мошенников необходимо знать следующее:

- сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты);

- хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте и не сообщать пин-код третьим лицам;

- помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС сообщении от банка;

- сотрудники банка никогда не попросят вас пройти к банкомату;

- остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;

- лучше избегать телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;

- внимательно читайте СМС сообщения приходящие от банка;

- никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;

- никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

- в сети «Интернет» не переходите по ссылкам на неизвестные сайты.

Куда обращаться, если мошенники вас обманули:

Если вы или ваши близкие столкнулись с аферистами, то как можно скорее обратитесь в ближайшее полиции и подайте заявление в полицию. Заявление составляется очень просто и является стандартным:

Данные заявителя, то есть ФИО, паспортные данные, фактический адрес проживания и контактный телефон.

Суть заявления. Представляет собой информацию о мошенниках в интернете, изложенную в свободной форме. Этот пункт должен содержать описание произошедшего со всеми подробностями.

Дата подачи заявления и подпись заявителя.