Памятка о способах мошенничества с использованием информационных технологий и методов социальной инженерии

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, МВД России, СК России, социальных служб или других официальных организаций.

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.

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.

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.

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.

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).

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.

Помните:

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. **Всегда перезванивайте в банк или организацию по официальным номерам в случае подозрительных звонков.**