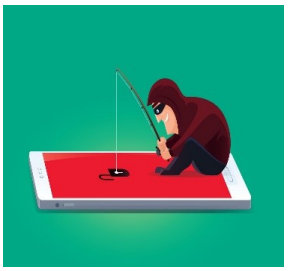
Прокуратура Авиастроительного района г.Казани разъясняет

Мошенничество в сфере информационно-телекоммуникационных технологий – это преступные действия, направленные на обман пользователей с целью получения их личных данных или денежных средств посредством использования современных технологий, таких как интернет и мобильная связь. С развитием цифровых технологий количество таких преступлений растет, и злоумышленники постоянно изобретают новые схемы обмана. Рассмотрим наиболее распространенные из них:

1. Фишинг

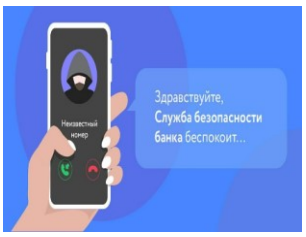


Фишинг — это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей, таким как логины, пароли или данные банковских карт. Мошенники рассылают электронные письма или сообщения в мессенджерах от имени известных брендов или организаций, содержащие ссылки на поддельные сайты, внешне неотличимые от настоящих. Попав на такой сайт и введя свои данные, пользователь передает их злоумышленникам.

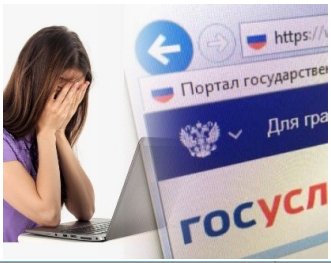
2. Вишинг

Вишинг (от англ. voice phishing) — это разновидность фишинга, при которой мошенники используют телефонную связь для обмана. Они звонят жертве, представляясь сотрудниками банка, полиции или другой организации, и под различными предлогами выманивают конфиденциальную информацию: номера банковских карт, пароли или коды подтверждения.

3. Сообщения и звонки от «сотрудников» организаций



Мошенники звонят или отправляют сообщения, представляясь сотрудниками правоохранительных органов, банков или государственных служб. Они сообщают о якобы возникших проблемах, например, попытке хищения денег с банковского счета, и предлагают перевести средства на «безопасный счет». После перевода деньги оказываются у злоумышленников.



4. Мошенничество через платформу «Госуслуги»

Злоумышленники звонят, представляясь сотрудниками портала «Госуслуги» или МФЦ, и сообщают о попытке взлома личного кабинета пользователя. Под предлогом защиты аккаунта они просят продиктовать коды из СМС или другие личные данные, что позволяет им получить доступ к аккаунту и оформить онлайн-кредиты на имя жертвы.

5. Поддельные интернет-магазины и сайты объявлений

Мошенники создают фальшивые интернет-магазины или размещают объявления о продаже товаров по привлекательным ценам. После получения оплаты товар не отправляется, или отправляется товар ненадлежащего качества. Также злоумышленники могут использовать фишинговые ссылки для кражи данных банковских карт.

6. Поддельные квитанции за коммунальные услуги

Мошенники рассылают поддельные квитанции за коммунальные услуги с указанием своих реквизитов. Оплачивая такие квитанции, граждане переводят деньги на счета злоумышленников.

<u>Рекомендации по защите от мошенничества</u>:

- **Бдительность:** Не доверяйте незнакомым звонкам и сообщениям, особенно если от вас требуют срочных действий или передачи личной информации.
- **Проверка информации:** При получении подозрительных сообщений или звонков свяжитесь с официальными представителями организаций по известным вам контактам для подтверждения информации.
- **Защита личных данных:** Никогда не сообщайте посторонним лицам свои персональные данные, пароли, PIN-коды или CVV-коды банковских карт.
- **Использование надежных паролей:** Создавайте сложные пароли для различных сервисов и регулярно их обновляйте.
- **Обновление программного обеспечения:** Регулярно обновляйте операционную систему и приложения на ваших устройствах, чтобы защититься от известных уязвимостей.
- **Использование антивирусных программ:** Установите и регулярно обновляйте антивирусное ПО на своих устройствах.
- **Проверка сайтов:** Перед вводом личных данных убедитесь, что сайт является официальным и защищенным (URL-адрес начинается с «https»).

Соблюдение этих рекомендаций поможет снизить риск стать жертвой мошенников и защитить ваши персональные данные и финансовые средства.