КИМРСКАЯ МЕЖРАЙОННАЯ ПРОКУРАТУРА

Памятка «Об основных способах дистанционного мошенничества»

Апрель 2025 г.

С развитием современных технологий в РФ наблюдается **рост дистанционного (телефонного) мошенничества**, которое посредствам мобильной связи, электронной почты, социальных сетей, онлайн- торговли и других цифровых сервисов предоставляет мошенникам, преследующим различные противоправные цели, широкие возможности для обмана отзывчивых и доверчивых граждан России.

Мошенники применяют различные **СПОСОБЫ** и **МЕТОДЫ** обмана людей, начиная от спама и заканчивая созданием сайтов-двойников.

Основная цель злоумышленников – получить **доступ** и **завладеть** персональными данными пользователей, например, паспортные данные, реквизиты банковских счетов, логины и пароли от социальных сетей.

Наиболее распространенные схемы дистанционного мошенничества

РОЗЫГРЫШЬ ПРИЗОВ

На телефон абонента сотовой связи приход SMS-сообщение, из его содержания следует, что в результате проведенного розыгрыша он **выиграл приз** (транспортное средство, квартиру, ценные бумаги и др.) и для получения подробной информации потенциальной жертве предлагается посетить сайт в сети «Интернет» и ознакомится с условиями получения выигрыша.

Далее мошенники сообщают, что нужно уплатить государственную пошлину

либо налог на выигрыш. После перевода денежных средств на счет получателя, мошенник требует от потенциальной жертвы ввести комбинацию цифр для проверки поступления денежных средств. После завершения этих действий счет жертвы обнуляется, и мошенник перестает выходить на связь.

ВАЖНО!

1. Изучите **правила розыгрыша**. Посмотрите кто его проводит, как и когда будут подведены итоги розыгрыша

2. Следите за **новостями** о розыгрыше в **официальном канале**

3. Не переходите по **непроверенным ссылкам**. **Не вводите** данные банковских карт в формах и вводах платежной информации

СЛУЧАЙ С РОДСТВЕННИКОМ

Мошенники звонят с незнакомого номера и выдают себя за родственника или знакомого и, использую взволнованный тон, сообщают по телефону, что его задержали сотрудники полиции за совершенное преступления. В разговор вступает человек, представляющийся сотрудником полиции, и говорит, что для освобождения задержанного необходимо перевести деньги на присланный банковский счет или передать лично определенному лицу для «решения проблемы».

ПОМНИТЕ!

Не следует доверять звонкам и сообщениям о том, что родственника или знакомого задержали **сотрудники полиции** или он попал в аварию, если после этого следует **просьба о перечислении денежных средств**

ФИШИНГ

В настоящее время одной из распространенных схем киберпреступников стал «Фишинг». Это вид мошенничества вынуждают потенциальных жертв с помощью **e-mailспама** или **рекламы** на не безопасных интернет- ресурсах заманивают на интернет - страницы, не отличимых по внешнему виду от **оригинальных сайтов банков**, интернет-магазинов, платежных систем, социальных сетей, требующих авторизации. Применяя различные психологические методы мотивации, злоумышленники подталкивают жертву самостоятельно ввести свои данные в формы поддельных сайтов.

ЗНАЙТЕ!

1. Получив письмо на электронную почту, не спешите на него отвечать. Обратите внимание на **адрес отправителя**

2. **Не вводите свои персональные данные** на неизвестных сайтах

3. В сети «Интернет» не переходите по ссылкам на **неизвестные сайты**