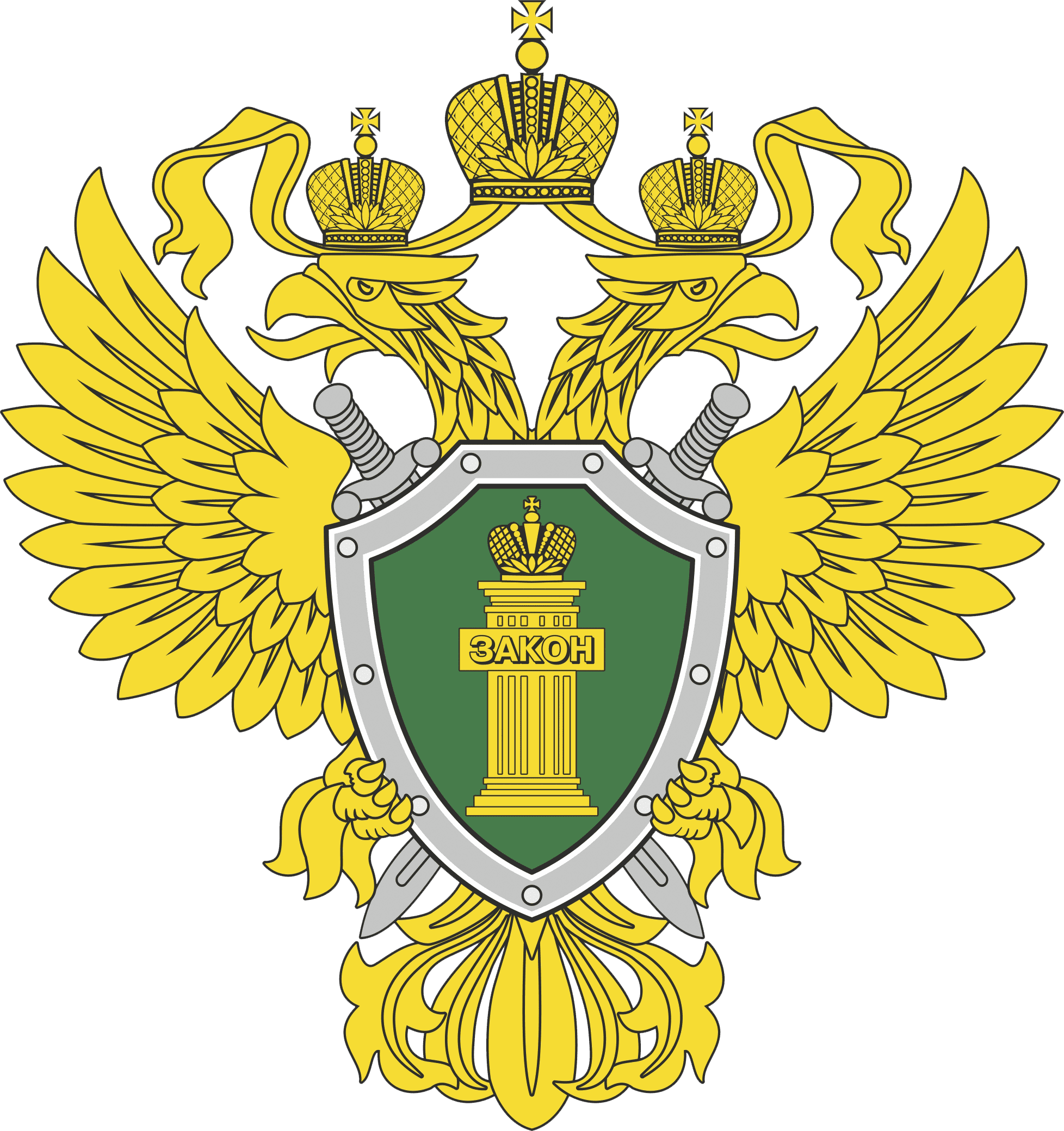
****

**Прокуратура Иланского района**

**ПАМЯТКА**

**Мошенничество в IT сфере**

**г. Иланский**

**2024**

***Как определить мошенничество***

***это незаконные действия, направленные на обман пользователей с целью получения доступа к их личным данным, финансовым средствам или ресурсам.***

***Главная цель — использовать полученную информацию для финансовой выгоды или нанесения ущерба.***

***Способы мошенничества***

***1. Фишинг: Метод обмана, при котором злоумышленники пытаются получить конфиденциальную информацию (например, логины, пароли, данные кредитных карт) под видом легитимных сообщений или сайтов.***

***2. Вишинг: Вид фишинга, который осуществляется через телефонные звонки. Мошенники могут представляться сотрудниками банков или иных организаций, чтобы получить персональные данные.***

***3. Смишинг: Форма фишинга с использованием текстовых сообщений (SMS) для того, чтобы завладеть личной информацией.***

***4. Поддельные сайты (клон-сайты): Создание фальшивых сайтов, которые имитируют легитимные сайты, с целью обманом заставить пользователей вводить личные данные.***

***5. Запросы на предоплату (advance-fee fraud): Мошенники убеждают пользователей в необходимости сделать предоплату за несуществующие товары, услуги или выигрыши.***

***6. Шпионское ПО (spyware): Программы, устанавливаемые на компьютеры без ведома пользователей для того, чтобы собирать личную информацию.***

***7. Малварь для вымогательства (ransomware): Вредоносные программы, которые блокируют доступ к данным пользователя до тех пор, пока не будет выплачен выкуп.***

***8. Обман в интернет-магазинах: Создание поддельных интернет-магазинов или использование легитимных платформ для продажи несуществующих товаров.***

***9. Киберсквоттинг: Регистрация доменных имён, сходных с известными брендами или компаниями, чтобы использовать их в мошеннических целях или продавать с наценкой.***

***Как не стать жертвой мошенников:***

**1. Не передавайте личные данные по телефону, особенно если вам звонят незнакомые люди.**

**2. Проверяйте информацию. Если вам звонят якобы из банка или другой организации, лучше завершить разговор и перезвонить по официальному номеру для уточнения.**

**3. Будьте осторожны с незнакомыми звонками. Если разговор кажется подозрительным или давят на вас психологически, лучше сразу положить трубку.**

**4. Используйте двухфакторную аутентификацию для защиты своих счетов и онлайн-аккаунтов.**

**5. Будьте осведомлены. Мошенники часто обновляют свои методы, и знание их схем может помочь избежать обмана.**

***Уголовная ответсвенность***

***Статья 159.6 УК РФ - Мошенничество в сфере компьютерной информации:***

***- Наказание: может наказываться штрафом, обязательными работами, а в более серьезных случаях — лишением свободы.***

***- Санкции: За мошенничество в крупном или особо крупном размере предусмотрено до 10 лет лишения свободы с возможным штрафом.***

***Статья 272 УК РФ - Неправомерный доступ к компьютерной информации:***

***- Наказание: Штрафы, обязательные работы, ограничение свободы или лишение свободы до 7 лет в зависимости от тяжести последствий.***



***Компьютерные мошенники играют на доверии, страхах и неосведомленности людей, поэтому важно сохранять бдительность и всегда перепроверять информацию.***



***В случае если вы стали жертвой мошенников в данной сфере, незамедлительно сообщите в***

******

***Прокуратуру Иланского района***

***ул. Коммунистическая,42, г. Иланский, 663800***

***Телефон +7 (39173)2-16-83***

***Электронная почта krpro126@24.mailop.ru***

***или***

***в правоохранительнын органы.***