****

**Прокуратура Рязанской области**

**ПАМЯТКА**

**ПРОФИЛАКТИКА**

**КИБЕРМОШЕННИЧЕСТВА**

****

**РЯЗАНЬ**

**2025**

1

**В Российской Федерации в настоящее время чрезвычайно актуальной является проблема кибермошенничества.**

**С помощью соцсетей, мессенджеров, цифровых устройств злоумышленники похищают денежные средства, получают несанкционированный доступ к личным данным.**

**Основные схемы обмана:**

* «Фишинг» (кража личной информации, такой как идентификатор клиента, PIN-код в Интернете, номер кредитной или дебетовой карты, дата истечения срока действия карты, номер CVV и т.д., через электронную почту)
* Звонки под видом работников банка, сотрудников правоохранительных органов под предлогом «защиты» денежных средств
* Размещение от имени родственников и знакомых просьб о переводе денежных средств в соцсетях и мессенджерах
* Фальшивые интернет-магазины с предложениями о продаже несуществующих товаров по низкой цене
* Предложения «легкого» заработка (инвестиций, ставок, курсов с гарантией дохода)

2

**Способы защиты:**

* Никогда не сообщайте PIN-коды, СVV банковских карт, коды из СМС-сообщений, паспортные данные
* Проверяйте полученную информацию: самостоятельно перезванивайте в банковские учреждения, внимательно сверяйте адреса предложенных сайтов (https, домены)
* Не переходите по подозрительным ссылкам
* Используйте сложные пароли и двухфакторную идентификацию
* Пользуйтесь антивирусным программным обеспечением
* Блокируйте подозрительные звонки и сообщения

**Жертвами киберпреступлений нередко становятся подростки.**

**Поэтому особенно важно:**

* Следить за онлайн-активностью ребенка
* Устанавливать родительский контроль и фильтры
* Обсуждать риски и правила поведения в сети Интернет
* Объяснять, как правильно реагировать на попытку обмана