**Информационный бюллетень**

**Парапинского сельского поселения**

**Ковылкинского муниципального района**

**Является официальным печатным**

**изданием Парапинского сельского**

**поселения Ковылкинского района**

**Республики Мордовия**

**От 01.11.2024г №47**

**Памятка для граждан об основных способах дистанционного мошенничества**

1. **Мошенничество по телефону**. Злоумышленники могут звонить под видом сотрудников банков, полиции, социальных служб или других официальных организаций. Они сообщают, что банковская карта или счёт подверглись атаке, и просят передать личные данные, одноразовые пароли или выполнить перевод средств.

**Что делать**: не передавать личные данные и пароли по телефону, завершить разговор и перезвонить в банк по официальному номеру. Никогда не совершать переводы по инструкциям незнакомцев.

1. **Фишинговые сайты и сообщения**. Это попытка получить личную информацию (пароли, данные карты) через поддельные сайты или сообщения, которые выглядят как настоящие.

**Что делать**: не переходить по ссылкам из подозрительных сообщений и писем, всегда проверять адрес сайта, прежде чем вводить данные. Использовать антивирусные программы, которые могут выявлять поддельные сайты.

1. **Мошенничество через мессенджеры и социальные сети**. Мошенники могут обращаться через мессенджеры или социальные сети, притворяясь друзьями, коллегами или представителями компаний.

**Что делать**: всегда проверять информацию, связавшись с человеком напрямую по телефону. Не переводить деньги по просьбам через мессенджеры.

1. **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 переходить по подозрительным ссылкам, особенно если предлагают «получить деньги». Использовать безопасные методы оплаты, проверять информацию о продавце, читать отзывы, не соглашаться на полную предоплату.

1. **Мошенничество с выигрышами и лотереями**. Мошенники часто используют фальшивые уведомления о выигрыше в лотереях или конкурсах, в которых человек не участвовал.

**Что делать**: если не участвовал в розыгрыше, быть уверенным, что это мошенничество. Никогда не переводить деньги и не предоставлять данные карты в обмен на обещание получения приза. Проверять информацию о конкурсах на официальных сайтах, а также читать условия розыгрышей.

1. **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 устанавливать ПО или не передавать доступ к устройству по запросам неизвестных. Если позвонили под видом технической поддержки, завершить звонок и обратиться в официальную службу поддержки через проверенные контакты.

**Основные рекомендации по защите от дистанционного мошенничества**:

* никогда не передавать личные данные, пароли и банковские реквизиты по телефону, в интернете или через SMS;
* быть бдительными к подозрительным предложениям, особенно если они связаны с деньгами или личной информацией;
* проверять достоверность сайтов, сервисов и организаций через официальные источники;
* использовать двухфакторную аутентификацию для защиты своих онлайн-аккаунтов;
* всегда перезванивать в банк или организацию по официальным номерам в случае подозрительных звонков.

**Если есть подозрения на мошенничество, рекомендуется обратиться в правоохранительные органы.**

Ковылкинская межрайонная прокуратура

**Информационный бюллетень Парапинского сельского поселения**

**Ковылкинского муниципального района № 47 от 01 .11.2024г.**

**Учредитель: Совет депутатов Парапинского сельского поселения Ковылкинского муниципального района**