ПРОКУРАТУРА ВОЛОГОДСКОЙ ОБЛАСТИ ПРЕДУПРЕЖДАЕТ

О новых способах дистанционного мошенничества

Злоумышленники с каждым разом используются все более изощренные способы «выманивания» денежных средств, а также личной информации, способствующей совершению хищений данных денежных средств, для чего используются различные жизненные ситуации, посредством которых на потерпевших оказывается воздействие с целью беспрепятственного завладения их денежными средствами.

Уважаемые граждане! Не устанавливайте незнакомые приложения и программы на свои персональные компьютеры и смартфоны, не вводите сведения о своих банковских картах на посторонних сайтах и приложениях, никому не сообщайте поступающие сведения из СМС-сообщений, не переходите по незнакомым ссылкам, исключите возможность оплаты через QR-код без проверки платежного документа на его действительность, не переводите свои денежные средства на посторонние банковские счета. Вышеуказанные меры позволят значительно снизить возможность хищения Ваших денежных средств.

Новые способы дистанционного мошенничества:

- **ПИСЬМА С ЗАДОЛЖЕННОСТЬЮ:** Злоумышленник рассылает гражданам письма с якобы существующими задолженностями из-за просроченных платежей по кредитным договорам и с угрозами за их неуплату арестом имущества.

В своих уведомлениях злоумышленники указывают сумму «задолженности», прилагая QR-код или ссылку для перехода к оплате, которую предлагается провести через систему быстрых платежей.

Иногда злоумышленники также предлагают скидки, которые якобы действуют непродолжительное время.

- **КВИТАНЦИИ ОБ УПЛАТЕ ШТРАФА ЛИБО КОММУНАЛЬНЫХ ПЛАТЕЖЕЙ:** Злоумышленник рассылает гражданам на электронную почту квитанции об оплате административного штрафа либо коммунальных платежей, которые незначительно отличаются от настоящих квитанций.

Оплатить данные квитанции предлагается через QR-код или реквизиты, указанные в квитанции.

- **ЗАМЕНА КЛЮЧА ОТ ДОМОФОНА:** Злоумышленник звонит гражданам, представляясь работником управляющей организации, и сообщает о замене входной двери в подъезд вместе с домофоном, и предлагает заменить ключи от домофона.

Согласно легенде злоумышленников, у каждой квартиры будет свой код от домофона, и именно он должен поступить гражданину в СМС-сообщении.

Для того, чтобы закодировать магнитные ключи, гражданам предлагается сообщить поступающие на их мобильный телефон СМС-коды.

После чего злоумышленники получают доступ к персональным аккаунтам граждан на портале «Госуслуги» со всеми их личными и банковскими данными.

- **ПРОСЬБА ПЕРЕЗВОНИТЬ:** Злоумышленники звонят гражданам и под различными предлогами упрашивают перезвонить по их номеру - это может быть СМС от «друга», звонок «сотрудника банка», «дальнего родственника» и тд.

Как в дальнейшем оказывается, эти номера относятся к номерной емкости интернет-сервиса, звонки на которые являются платной услугой.

Граждане перезванивают на данные номера, их держат на линии под различными предлогами, а с баланса абонентского номера списываются все денежные средства.

- **ПРЕДЛОЖЕНИЕ ВОССТАНОВИТЬ БАНКОВСКИЕ КАРТЫ:** Злоумышленники отправляют гражданам СМС-сообщения с предложением восстановить банковские карты Visa и Mastercard.

В данных сообщениях прикреплена ссылка, по переходу на которую гражданам предлагается ввести реквизиты своих банковских карт.

После введенных данных злоумышленники получают доступ к банковским картам граждан.

- **ЗАПИСЬ НА ПРИЕМ К ВРАЧУ:** Злоумышленники отправляют гражданам СМС-сообщения либо звонят и сообщают им о записи на прием к врачу.

Для подтверждения записи граждан просят продиктовать поступивший им на телефон код из СМС-сообщения.

После чего злоумышленники получают доступ к персональным аккаунтам граждан на портале «Госуслуги» со всеми их личными и банковскими данными.

- **ЗАДОЛЖЕННОСТЬ ПО НАЛОГАМ:** Злоумышленники звонят гражданам и представляются сотрудниками налоговой службы.

В ходе разговора гражданам сообщают о том, что у них обнаружены скрытые доходы, за которые не уплачены налоги.

Для того, чтобы лицо не привлекать к ответственности за неуплату налогов и не изымать имущество в пользу государства злоумышленники предлагают срочно оплатить образовавшуюся задолженность через поступивший на телефон гражданина QR-код.

- **ИСТЕК СРОК БЕСПЛАТНОГО ХРАНЕНИЯ ТОВАРА**: Злоумышленники звонят гражданам, представляясь работниками интернет-магазинов, и сообщают о том, что истек срок бесплатного хранения товара.

Для того, чтобы отказаться от заказа, злоумышленники предлагают гражданам сообщить поступивший им на мобильный телефон код из СМС-сообщения.

После чего злоумышленники получают доступ к персональным аккаунтам граждан на портале «Госуслуги» со всеми их личными и банковскими данными.

- **ЗАКАЗНОЕ ПИСЬМО:** Злоумышленники звонят гражданам, представляясь работниками АО «Почта России» и сообщают о поступлении в почтовое отделение заказного письма на имя граждан.

Получателям письма предлагают вариант получения его на электронную почту, для чего необходимо назвать поступивший им на мобильный телефон код из СМС-сообщения.

- **ПРИЛОЖЕНИЕ ДЛЯ ОПЛАТЫ КОММУНАЛЬНЫХ УСЛУГ:** Злоумышленники звонят гражданам и предлагают для удобства скачать приложение для оплаты коммунальных услуг.

Граждане, ничего не подозревая, следуя их инструкциям скачивают и устанавливают приложения на свой мобильный телефон.

Как в дальнейшем оказывается, установленное приложение позволяет злоумышленникам получить доступ к телефонной книге граждан, их мобильным банкам и другим личным данным.

- **ПОЛУЧЕНИЕ НОВОГО ПОЛИСА ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ:** Злоумышленники звонят гражданам и сообщают им о том, что на их имя выпущен новый полис обязательного медицинского страхования.

Гражданам сообщают, что забрать его можно в ближайшем отделении многофункционального центра.

Для того, чтобы определить, какой многофункциональный центр находится в непосредственной близости от граждан, необходимо сообщить поступивший им на мобильный телефон код из СМС-сообщения.

После чего злоумышленники получают доступ к персональным аккаунтам граждан на портале «Госуслуги» со всеми их личными и банковскими данными.

Прокуратура Вологодской области

О новых способах дистанционного мошенничества

г. Вологда, 2025