РЕСПУБЛИКА ДАГЕСТАН
АДМИНИСТРАЦИЯ
ГОРОДСКОГО ОКРУГА
«ГОРОД ЮЖНО-СУХОКУМСК»

368890, г. Южно-Сухокумск, ул. им. Гаджи Махачева 13, Тел/факс
(87276) 2-10-10, E-mail: goyuzhno-suxokumsk@mail.ru

«03» 05 2025 г. № 436-11

На _____ от _____2025 г.

Руководителям предприятий,
учреждений и организаций в
ГО «г. Южно-Сухокумск»
(по списку)

Уважаемые руководители!

В целях предупреждения и минимизации фактов совершения дистанционных краж и мошенничества направляем в Ваш адрес «Информационную памятку по профилактике мошеннических действий». Просим в обязательном порядке довести данную информацию до сотрудников Ваших предприятий, учреждений, организаций (далее - ПУО). В целях повышения эффективности профилактики киберпреступности и проведения максимально широкой информированности населения рекомендуем разместить данную информацию в официальных аккаунтах ПУО в сети Интернет.

Приложение: Информационная памятка на 2 л.

Глава городского округа
«город Южно-Сухокумск» **С.С. Мамадов**

Исп. Шахманов Г.Г.
8(87276) 2-13-27

Информационная памятка
по профилактике мошеннических действий!

Напоминаем, что с информацией о новых видах и способах дистанционных мошенничеств можно ознакомиться на официальных аккаунтах «Вестник Киберполиции России» в социальных сетях «Одноклассники» (https://ok.ru/group/70000008643680), в агрегаторе новостей «Дзен» (https://dzen.ru/id/66f3a635b44c3033e86bf6ce), а также в социальной сети «Вконтакте» (https://vk.com/cyberpolice_rus).

Будьте бдительны! Ежедневно финансовые аферисты придумывают новые способы мошенничества.

1. «Безопасный счет», звонки мошенников, которые представляются должностными лицами налоговой службы, полиции, ФСБ, прокуратуры, Пенсионного фонда, Госуслуг и др.

Его подвиды:

- «предоставление доступа к экрану телефона с последующим входом в различные приложения и хищением денежных средств»;

- «представление сотрудником госорганизации, оказывающей помощь по возврату ранее похищенных денежных средств»;

- «замена электросчетчика, установка соответствующего приложения в телефон и предоставление кодов из СМС»;

- «продление договоров обслуживания сим карт мобильных операторов связи, под предлогом улучшения качества связи» вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей или банковским реквизитам;

- «представление агентом страховой компании для перерегистрации медицинской страховки путем предоставления кодов по СМС»;

- «неоднократные звонки с разных номеров с информированием о взломе (попытки взлома) личного кабинета «Госуслуг», оформлением кредитов, переводом денежных средств на безопасный счет».

2. «Инвестиции» под видом финансовых экспертов мошенники в интернете рассказывают об уникальной схеме заработка.

3. «Заказ товаров в интернете, в том числе через сайты бесплатных объявлений Авито, Юла, Яндекс для продажи товаров и оказания услуг по подозрительно низкой цене».

4. «Взлом социальных страниц»

5. «Манипуляции под видом какого-либо крупного выигрыша».

6. «Родственник попал в ДТП, сбил человека и др.» мошенник под видом родственника, попавшего в ДТП, либо сотрудника правоохранительных органов просит деньги за возможность избежать наказания за противоправное деяние.

Ущерб, нанесенный физлицам действиями мошенников, за первую половину 2024 г. составил 91 млрд руб. За полный 2023 г. мошенники украли у граждан 157 млрд руб. Рост кибератак за последние три года, по информации следственного департамента МВД России, составил 27%.

Чтобы не оказаться жертвой мошенников необходимо знать следующее:
- избегайте телефонных разговоров с подозрительными людьми, не бойтесь прервать разговор, просто кладите трубку;

- ни при каких обстоятельствах не сообщайте данные вашей банковской карты, а также секретный код на оборотной стороне карты;

- остерегайтесь «телефонных» мошенников, которые под видом сотрудником МВД, ФСБ, Центробанка и т.д. пытаются запугать Вас привлечением к уголовной ответственности, штрафами;

- никогда и никому не сообщайте пароли и секретные коды, которые приходят вам в СМС сообщении, и помните, что только мошенники их запрашивают;

- не покупайте в интернет - магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;

- в сети «Интернет» не переходите по ссылкам на неизвестные сайты;
- не передавайте деньги неизвестным лицам для решения возникших у Вас якобы проблемных вопросах;

- никогда не переводите денежные средства, если об этом вас просит сделать Ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

- если Вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;
- при смене номера телефона, отключите от него все мобильные банки и прочие сервисы, дающие доступ к Вашим финансам.