**Брифинг по вопросам информационной безопасности.**

**Временно исполняющий обязанности начальника МО МВД «Нижнесергинский» майор полиции И.Р. Даутов провёл встречу с прессой.**

На прошлой неделе состоялась важная информационно-профилактическая встреча с представителями прессы Нижнесергинского района, посвящённая вопросам кибербезопасности и защите граждан от современных мошеннических схем. Её инициатором и ведущим стал Ильдар Раисович Даутов.

Повышение киберграмотности ключ к защите. Мероприятие прошло в рамках Всероссийской информационно-профилактической кампании МВД России, цель которой противодействие киберпреступности и повышение уровня осведомлённости населения о современных методах мошенничества.

Ильдар Даутов подробно рассказал журналистам о наиболее распространённых схемах обмана, применяемых злоумышленниками с использованием информационно-коммуникационных технологий и телефонной связи.

**Основные схемы обмана населения.**

Мошенники нередко выдают себя за сотрудников банков или полиции, утверждая, что со счетов граждан пытаются украсть сбережения. Для «безопасности» предлагают перевести деньги на «специальный защищённый счёт», после чего жертвы теряют свои средства и зачастую оформляют кредиты. Распространены звонки якобы от налоговой службы, страховых компаний, ЖКХ, Госуслуг, пенсионного фонда и других организаций.

Например, мошенники, представляясь «представителями Госуслуг», требуют назвать код из СМС, чтобы получить доступ к личному кабинету и забрать личные данные. Звонки от «Пенсионного фонда» включают обман о положенных выплатах с просьбой сообщить реквизиты карты, включая код с обратной стороны. При звонках якобы от «Центробанка» предлагают скачать приложение «Банкноты Банка России», которое на деле содержит вредоносное программное обеспечение. Лжесотрудники «медицинских учреждений» сообщают о дефицитных лекарствах и просят оплатить их при помощи банковской карты.

« О п е р а т о р ы с в я з и »звонят с сообщениями об истечении срока действия SIM-карты, получая доступ к личному кабинету через СМС-коды.  Звонки от «потенциальных покупателей» по объявлениям в интернете предусматривают выманивание реквизитов банковских карт с дальнейшими хакерскими атаками. Обещания «лёгкого заработка» и «крупных выигрышей» маскируют попытки получения личных данных и денежных переводов. Сообщения о том, что родственник попал в беду, используются для запугивания и выманивания денег.

**Правила защиты от мошенничества.**

В финале встречи Ильдар Даутов рассказал о том, как можно защитить себя и своих близких от мошеннических действий.

 Никогда не переводите деньги незнакомцам. Самый безопасный для гражданина счёт — его счёт в банке.

 Не передавайте пароли, ПИН-коды, данные паспортов и номер карты третьим лицам.

 Никогда не сообщайте код с обратной стороны карты и СМС-коды.

 Не доверяйте подозрительным звонкам — банки и полиция не запрашивают такие данные.

 Не скачивайте приложения из непроверенных источников.

 При онлайн-покупках используйте только проверенные магазины и платежные системы.

 Блокируйте подозрительные номера.

 Согласуйте с близкими «контрольный вопрос» для проверки звонков.

 При подозрении на мошенничество сразу обращайтесь в полицию и банк.

Ильдар Раисович также привёл конкретные примеры мошеннических действий, зафиксированных в Свердловской области, включая Нижнесергинский район и Бисертский муниципальный округ. Всем участникам встречи были предоставлены тематические памятки с рекомендациями по защите. Данная встреча стала важным шагом в системной работе МВД по повышению информированности населения о современных угрозах и методах защиты от кибермошенничества. Полученные знания помогут гражданам быть более бдительными и защищёнными в цифровом пространстве, снижая риски финансовых потерь и сохранения личной безопасности.