Информация
по профилактике мошенничества с использованием информационно-телекоммуникационных технологий

За 11 месяцев 2024 года в УМВД России по г. Н.Новгороду зарегистрировано 4574 преступления по линии мошенничества и отдельным видам краж, в том числе совершенных с использованием информационно-телекоммуникационных технологий. Общий ущерб, причиненный гражданам, составил свыше 1,5 миллиардов рублей.

Полиция Нижнего Новгорода регистрирует различные способы совершения мошенничеств, к наиболее распространенным схемам обмана можно отнести следующие:

1. Злоумышленники звонят под видом сотрудников служб безопасности банков, государственных организаций (МФЦ, Госуслуги, правоохранительные органы и т.п.), операторов сотовой связи, которые различными способами убеждают потерпевших переводить денежные средства на расчетные счета и абонентские номера. Следует отметить предлоги, которые используют мошенники:

- информация о подозрительных операциях, совершаемых с использованием счетов потерпевших (с целью получения их персональных данных и банковских реквизитов) - ***(60-летняя жительница Сормовского района после телефонных звонков в одном из мессенджеров перевела на разные расчетные счета 3 560 000 рублей, 3 000 000 из которых оформлены в кредит).***

- информация об оформлении третьими лицами на потерпевшего кредита на крупную сумму (в целях предотвращения незаконной операции гражданина убеждают самостоятельно оформить кредит на такую же сумму, которую впоследствии требуется перевести на так называемый «безопасный счет») - ***(59-летняя нижегородка в течение 3 месяцев по указанию телефонных собеседников, представлявшихся сотрудниками различных структур, продала две квартиры и оформила несколько кредитов под залог автомобилей, потеряв в общей сложности 29,7 млн рублей).***

- информация о якобы взломе личного кабинета портала «Госуслуг» (с целью получения установочных данных, преступники входят в сервис, получают сведения о документах, бюро кредитных историй и оформляют кредиты дистанционным способом) – (***27-летняя жительницы Ленинского района после общения с сотрудником поддержки сайта «госуслуг» обналичила собственные и кредитные 2 660 000 рублей и перевела на указанные злоумышленником реквизиты).***

- информация о прекращении обслуживания сим-карты (продление договора об оказании услуг связи происходит после получения от потерпевшего смс-кодов и паролей от портала «Госуслуг») - (***под предлогом подключения тарифа на выгодных условиях, злоумышленники вынудили 64-летнюю жительницу Нижегородского района сообщить СНИЛС и скачать***

приложение удаленного доступа, после чего с кредитной карты похитили 130 000 рублей).

В целях недопущения подобных преступлений необходимо сохранять бдительность при поступлении телефонных звонков от представителей вышеперечисленных организаций. Никому не передавайте реквизиты своих банковских карт, пароли от платежных систем или личных страниц на сайтах государственных органов. Не совершайте финансовых операций по указанию неизвестных лиц.

2. Еще один способ обмана граждан, когда по телефону сообщают о нарушении их родственниками действующего законодательства (совершение ДТП, причинение телесных повреждений, хранение наркотиков и т.п.), с целью передачи потерпевшими денежных средств через посредников, либо перевод их через терминалы оплаты для разрешения сложившейся ситуации. При этом мошенники стараются держать «жертву» всегда на связи с целью исключения каких-либо действий с ее стороны по проверке информации. ***(92-летняя пенсионерка в Советском районе отдала курьеру 1 070 000 рублей, после звонка якобы о дорожной аварии с ее братом)***.

Рекомендуется регулярно проводить беседы с пожилыми родственниками, которые чаще всего становятся жертвами данного вида обмана. Главное правило защиты – прекратить диалог и незамедлительно связаться с родственником, о котором шла речь, либо с кем-то из близких.

3. Осуществление звонков от имени представителей инвестиционных компаний с предложением получения крупных сумм от инвестирования при минимальных вложениях, а также при игре на бирже. Лжеброкеры консультируют и руководят действиями жертвы по открытию инвестиционных счетов, получая необходимые данные для осуществления его контроля. Подобный вид мошенничества может длиться продолжительное время, пока потерпевший не решается осуществить вывод денежных средств, который самостоятельно сделать не может. Кроме того, данное обстоятельство мошенники могут использовать с целью получения с потерпевшего дополнительных денег (например, для вывода полученных дивидендов, необходимо оплатить налог, комиссию и т.п). ***(В Нижегородском районе 39-летний мужчина под предлогом заработка на бирже лишился 4 732 000 рублей, как кредитных, так и личных.)***

Помните, что реклама подобных предложений, как правило очень навязчивая, сулит максимально высокий доход при минимальных временных затратах. Инвестированием необходимо заниматься, посоветовавшись лично с людьми, знакомыми с этой сферой деятельности.

Лучшая защита от телефонного мошенничества не отвечать на звонки от неизвестных номеров.

4. Мошенники могут использовать в качестве обмана смс-сообщения якобы от имени руководителя организации или контролирующего ведомства. Предупредив гражданина о том, что необходимо выполнять все требования, которые в последующем будет диктовать звонивший. Злоумышленники

взламывают аккаунты в мессенджерах, либо используют фейковые номера телефонов. ***(В Нижегородском районе 79-летняя женщина, получив звонок от якобы руководителя с сообщением о том, что с ней свяжутся из службы безопасности, под предлогом отмены несанкционированных операций по банковскому счету перевела личные 2 500 000 рублей на указанные реквизиты).***

В данном случае, получив подобное сообщение, рекомендуется позвонить адресату по номеру, записанному в ваших контактах. Не вступать в переписку и не выполнять указания, связанные с финансовыми операциями. Важно знать, что в настоящее время в данной схеме мошенничества злоумышленники могут применить искусственный интеллект, используя который можно клонировать голос определенного лица.

5. Покупки в сети Интернет также используются преступниками для хищения денег у граждан. Когда покупатель или продавец на сайте бесплатных объявлений получает подложную ссылку и оплачивая покупку товара или курьерские услуги, в последствии обнаруживает заблокированное объявление. (***45-летний житель Советского района, покупая снегоход по онлайн-объявлению, оплатил его покупку в размере 1 591 000 рублей, после чего лжепродавец его заблокировал. В Московском районе 24-летняя девушка потеряла 90 000 рублей, покупая билеты на концерт по подложной ссылке).***

Не стоит перечислять деньги за товар, не изучив отзывы о продавце/покупателе, а также сайте интернет-магазина. Если для обсуждения условий сделки предлагается перейти в мессенджеры – скорее всего это мошенники. Никогда не осуществляйте 100% оплату приобретаемого товара.