Информация
о появлении новых и наиболее распространенных способах совершения дистанционных мошенничеств

В целях повышения эффективности профилактики киберпреступности и проведения информационно-просветительской работы среди населения Главное управление МВД России по Челябинской области информирует о появлении новых и наиболее распространенных способах совершения дистанционных мошенничеств.

По итогам 9 месяцев 2024 года ущерб от преступлений, совершенных с использованием информационно-коммуникационных технологий составил 2 млрд 664 млн рублей.

В настоящее время появились и распространяются следующие виды мошеннических действий под условным наименованием:

1. «Выпуск электронного полиса обязательного медицинского страхования». Злоумышленник представляется работником медицинской организации либо страховой компании (занимающейся медицинскими страховками) и сообщает о необходимости замены полиса обязательного медицинского страхования на электронный. Для подтверждения выпуска такого полиса потенциальную жертву просят перейти по направляемой (предоставляемой) ссылке для подтверждения согласия, а также назвать код из SMS-сообщения.

2. «Подано исковое заявление в суд». Злоумышленники звонят гражданину под видом некого «помощника судьи» и сообщают, что в отношении него подано исковое заявление и, чтобы ознакомиться с документами, необходимо получить доступ через специальный портал. Для регистрации на данном портале необходимо перейти по направляемой (предоставляемой) ссылке.

Совершение таких действий приводит к утрате контроля над персональными, конфиденциальными данными и соответствующим рискам совершения киберпреступлений.

Помимо указанных способов мошенничеств, наиболее актуальными и используемыми схемами дистанционных посягательств остаются:

1. Злоумышленник представляется сотрудником банка, полиции, прокуратуры, ФСБ, Следственного комитета. Используя методы психологического манипулирования и пользуясь доверчивостью, злоумышленник вынуждает потерпевшего сообщать персональные данные, сведения о финансовом состояния, наличии автотранспорта в собственности. Затем, находясь под психологическим воздействием мошенника, потерпевший переводит денежные средства на якобы безопасные расчетные счета[1].

2. Злоумышленник, маскируясь под представителя оператора связи, убеждает потенциальную жертву посягательства, что срок действия sim-карты для использования мобильной связи истекает. Для продления ее работы необходимо сообщить код из присылаемого SMS-сообщения. Такое действие обеспечивает

[1] В отдельных случаях, переводятся средства, вырученные от срочной продажи автотранспорта или недвижимости. Причем сделку по срочной продаже имущества могут организовать сами мошенники. Как в этой схеме совершения посягательств, так и в последующих, потерпевшими могут стать все категории граждан, независимо от пола, образования, экономического, национального, социального статуса, а также возраста.

возможность подключения переадресации звонков и SMS-сообщений на другой телефонный номер и получение доступа к онлайн-банкингу, социальным сетям и мессенджерам потерпевшего для входа по номеру телефона.

3. Совершение посягательства под предлогом оказания содействия родственнику, якобы попавшему в дорожно-транспортное происшествие или задержанному правоохранительными органами. Введенный в заблуждение человек передает денежные средства прибывшему к нему курьеру, который в дальнейшем перечисляет полученные денежные средства на указанные мошенниками банковские счета (при этом оставляя себе определенный процент средств).

4. Еще одной распространенной мошеннической схемой остается предложение дополнительного заработка, участия в торгах на бирже, а также инвестирования в различные ценные бумаги. Граждан заманивают яркими вывесками, наименованиями, созвучными с названиями крупных нефте-газодобывающих компаний и холдингов, так называемыми «исключительными» предложениями и возможностью получения высокого дохода, в том числе за короткий промежуток времени. Попавшего под воздействие указанных факторов человека вынуждают вносить крупные суммы денежных средств, без возможности их вывода в дальнейшем.

5. Совершение мошеннических действий с использованием популярных торговых интернет-площадок объявлений о купле-продаже различного имущества или оказания услуг путем размещения «фиктивного» объявления о продаже товара по цене значительно ниже рыночной. Как правило, переписка между покупателем и мошенником ведется на торговой площадке либо с использованием интернет-мессенджеров. В ходе общения мошенник входит в доверие и вынуждает потерпевшего оплатить товар полностью либо внести определенную предоплату путем электронных переводов. После оплаты контакты с покупателем как правило прекращаются, его блокируют, объявление удаляют.

6. Мошенничество под условным наименованием «Перерасчет пенсии». В процессе телефонного разговора злоумышленники сообщают потенциальной жертве о якобы неучтенном стаже, выявленном в ходе некой проверки, в связи с чем предлагают оформить официальное заявление на перерасчет пенсии для ее увеличения. В случае согласия с такой процедурой мошенники предлагают подать заявление в телефонном режиме. Для идентификации просят продиктовать поступивший код из SMS-сообщения. Если сообщить данный код, то мошенники получат доступ либо к интернет-порталу «Госуслуги», либо к приложению мобильного банка, что приведет к компрометации учетной записи на «Госуслугах» или попытке перевода денежных средств с банковского счета жертвы.

Главное управление МВД России по Челябинской области