

Информация

о наиболее распространенных способах совершения преступлений с использованием информационно-коммуникационных технологий

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

На территории Челябинской области сотрудниками органов внутренних дел ежедневно фиксируются факты совершения дистанционных посягательств. В 2025 году зарегистрировано свыше 11,2 тыс. краж и мошенничеств, совершенных с использованием коммуникационных технологий. Совокупный ущерб от таких посягательств превысил 3,2 млрд рублей.

Для совершения преступлений мошенники используют методы социальной инженерии и психологического манипулирования, воздействуют на эмоциональную сферу человека, стремясь вызвать чувство тревоги, необходимости срочности совершения тех или иных действий, а также определенного доверия к якобы «официальному» источнику сообщаемой информации. Такие воздействия ослабляют рациональный контроль и заставляют потерпевших действовать импульсивно, например, сообщать конфиденциальные данные, переводить денежные средства, совершать электронные платежи или оформлять кредит.

Соответственно для эффективной профилактики преступлений, совершаемых с использованием коммуникационных технологий, необходима информационно-разъяснительная работа, направленная на повышение уровня осведомленности населения о методах совершения киберпреступлений.

В настоящее время распространяются следующие виды противоправных действий:

1. Мошенничество под предлогом дополнительного заработка, инвестирования. При таком способе совершения посягательства злоумышленники представляются финансовыми брокерами или сотрудниками инвестиционных платформ, в том числе используют наименования известных компаний: «Vinapse», «ГазпромИнвест», «Тинькофф Инвестиции» и др. Гражданам предлагают участие в инвестиционных проектах, обещая высокий доход и «гарантированную прибыль». После внесения денежных средств потерпевшие теряют доступ к своим счетам, а связь (контакты) со злоумышленниками прекращается.

Как в этой схеме совершения преступления, так и в других, потерпевшими могут стать граждане разных возрастов и социальных категорий, в том числе имеющие опыт пользования финансовыми сервисами.

2. Злоумышленник представляется сотрудником кредитно-финансовых учреждений и (или) правоохранительных органов. Используя методы

психологического манипулирования и пользуясь доверчивостью, он предлагает «защитить» денежные средства или якобы предотвратить оформление кредита на жертву посягательства. Затем, находясь под психологическим воздействием мошенника, потерпевшего убеждают перевести денежные средства на некие «безопасные расчетные счета». В отдельных случаях предлагают переводить средства, вырученные от срочной продажи автотранспорта или недвижимости.

Основная цель такой схемы совершения преступления - получить доступ к личным данным человека, реквизитам его банковских карт и средствам на счетах.

3. Мошенничество, совершаемое с использованием Единого портала государственных и муниципальных услуг (далее - портал «Госуслуги») и SIM-карт (идентификационный электронный модуль абонента, применяемый для обеспечения мобильной связи).

В этом случае злоумышленник, маскируясь под представителя оператора связи, убеждает потенциальную жертву посягательства, что срок действия SIM-карты для использования мобильной связи истекает и сообщает о необходимости продления договора на обслуживание номера. Под этим предлогом жертву просят сообщить код из присылаемого SMS-сообщения, который фактически является кодом для входа в личный кабинет на портале «Госуслуги». После того как мошенники получают код и, соответственно, доступ к учетной записи человека, они изменяют контрольные данные. Войдя в учетную запись, мошенники могут оформить кредит на потерпевшего, подать заявление на налоговый вычет или совершить иные действия от имени потерпевшего.

Так как код из SMS-сообщения подтверждает личность пользователя и может использоваться для верификации (процесс проверки и подтверждения достоверности чего-либо) и доступа к учетной записи на портале «Госуслуги», он является главной целью мошенников и одновременно значимым элементом обеспечения информационной безопасности, не предназначенным для разглашения неизвестным лицам.

Одним из распространенных в настоящее время предложений для получения такого кода является мошенническое предложение о записи на прием в государственные структуры. Для этого злоумышленники рассказывают о возможности «перерасчета» пенсии, изменении тарифов жилищно-коммунальных услуг, неких ошибках в налоговой декларации и других поводах, после чего, для фиктивной записи, просят назвать присылаемый код из SMS-сообщения.

Важно помнить, что для подтверждения записи на прием в государственные органы SMS-верификация не используется. Запись осуществляется исключительно через официальные интернет-сервисы или портал «Госуслуги», без передачи каких-либо кодов по телефону или в популярных мессенджерах.