АДМИНИСТРАЦИЯ ГОРОДА ЧЕЛЯБИНСКА
КОМИТЕТ ПО ДЕЛАМ ОБРАЗОВАНИЯ ГОРОДА ЧЕЛЯБИНСКА
ул. Володарского, д. 14, г. Челябинск, 454080, тел./факс: (8-351) 700-18-01, e-mail: edu@cheladmin.ru

09 НОЯ 2023 № 07/9176

На № _____ от _____

Директору МКУ «ЦОДОО г.Челябинска»
Сычевой А.А.

Начальникам СП МКУ «ЦОДОО г.Челябинска»

Руководителям образовательных учреждений

Уважаемые руководители!

Направляем для руководства и использования в работе Информацию о наиболее распространенных способах совершения преступлений с использованием информационно-телекоммуникационных технологий (письмо Министерство общественного безопасности Челябинской области от 02.11.2023 № 8570).

Информация, содержащаяся в указанном письме может быть применены для проведения информационно-просветительсткой работы в трудовых коллективах, родителями учащихся и создания информационного контента.

Приложение на 2 л. в 1 л.

Председатель Комитета

Комитет по делам образования города Челябинска
Документ подписан Электронной подписью
Сведения о сертификате ЭП
Кому выдан: Портье Светлане Викторовне
Серийный номер: 00 d5 e9 23 78 ff b9 ae 83
Срок действия: 16.05.2022 - 15.05.2027

С. В. Портье

М. А. Кинёва
700 18 70
Рассылка: МКУ «ЦОДОО», СП МКУ «ЦОДОО», ЦРО для рассылки во все ОУ

Информация
о наиболее распространенных способах совершения преступлений с использованием информационно-телекоммуникационных технологий

ГУ МВД России по Челябинской области информирует о наиболее распространенных способах совершения дистанционных мошенничеств:

1. Злоумышленник представляется сотрудником банка, полиции, прокуратуры, ФСБ, Следственного комитета, используя IP-телефонию звонит потерпевшему с подменных номеров[1] и информирует гражданина о подозрительных финансовых операциях по его банковскому счету, попытках оформления кредита, перевода денежных средств с его счета, либо сообщает о розыске, задержании преступников, совершающих хищения денежных средств с расчетных счетов граждан, при этом извещает о необходимости соблюдения некой «тайны следствия».

Далее, 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[2].

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 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 предлог 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.

[1] Номерная емкость начинается с 8800, 495, 499, а также с использованием номеров телефонов реально существующих ведомств, организаций, государственных органов, применяя специальное оборудование и программное обеспечение.

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

5. Совершение мошеннических действий с использованием популярных торговых интернет-площадок объявлений о купле-продаже различного имущества или оказания услуг путем:

5.1. 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 популярных 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.

5.2. Хищения денежных средств под предлогом приобретения товара у потенциальной жертвы. В данном случае переписка между продавцом и мошенником также ведется с использованием сообщений на сайте, либо с использованием мессенджеров. Продавца убеждают направить товар популярными интернет-сервисами доставки, в том числе используемыми на торговых площадках, сообщая, что товар оплачен, и для получения денежных средств необходимо перейти по ссылке, которую присылают на телефон продавца.

После перехода по ссылке продавец попадает на фишинговый сайт, аналогичный официальному сайту торговой площадки, где вносит свои персональные данные, реквизиты банковской карты и необходимую сумму. После нажатия на «окно» «Получить деньги», денежные средства списываются с расчетного счета продавца. В дальнейшем мошенники убеждают продавца, что произошел некий сбой и для возврата денежных средств необходимо обратиться в службу поддержки, перейдя по еще одной присылаемой ссылке. Продавец, перейдя по ссылке, вновь попадает на фишинговый сайт, где повторно указывает свои данные, реквизиты карты и сумму, якобы необоснованно списанную. После нажатия на «окно» «Получить деньги» с расчетного счета продавца повторно списываются денежные средства.

Аналогичным способом совершается хищение денежных средств через сервис по поиску попутчиков: мошенники размещают объявления с предложением услуги по пассажирским перевозкам. Когда пользователь откликается на объявление, мошенник в чате официального сайта поиска попутчиков просит его связаться с ним через популярный мессенджер по определенному номеру телефона. Затем, в ходе переписки клиенту предлагают оплатить поездку заранее и скидывают ему для этого ссылку на фишинговый сайт для оплаты. После перехода на сайт, пользователь вводит реквизиты своей банковской карты, далее денежные средства списываются на счет мошенникам.

6. Распространение получила схема хищения денежных средств с использованием социальных интернет-сетей. Якобы от имени потерпевшего его знакомым, друзьям, родственникам приходит сообщение с просьбой одолжить денежные средства. Также злоумышленники с использованием популярных мессенджеров рассылают сообщение о сборе денежных средств на лечение больного ребенка, похороны и т.д.

7. Действует преступная схема с оформлением кредита в микрофинансовых организациях без ведома потерпевшего. Хищение осуществляется путем перебора сим-карт для поиска активного аккаунта заемщика и использование личного

кабинета лица, ранее оформлявшего в микрофинансовых организациях заем.

8. Еще одним способом остается совершение противоправных деяний под предлогом получения возврата (компенсации) денежных средств за ранее приобретенные биологически активные добавки (БАДы). Мошенники, представляясь сотрудниками правоохранительных органов, в телефонном разговоре с потерпевшим сообщают, что задержали преступников, занимавшихся ранее продажей некачественных пищевых добавок. Для получения компенсации необходимо оплатить налог, открыть счет, совершить транзакцию и т.п. В результате граждане, рассчитывая получить компенсацию, перечисляют мошенникам денежные средства, сумма которых превышает сумму обещанной компенсации.

ГУ МВД России по Челябинской области