Прокуратура Ивановской области

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по профилактике преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Наиболее распространенные способы дистанционных мошенничеств.

Как не стать жертвой мошенничества.

2025

Анализ криминогенной обстановки на территории области свидетельствует об увеличении в 2024 году количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий (далее — ИТТ), снижении их раскрываемости.

В 2024 году на территории Ивановской области зарегистрировано 4352 преступления, совершенных с использованием информационно-телекоммуникационных технологий. Из общего количества зарегистрированных преступлений составляют мошенничества (ст. 159 УК РФ) – 2114, неправомерный доступ к компьютерной информации (ст. 272 УК РФ) – 374.

Под киберпреступностью понимается незаконная деятельность, в рамках которой атакуются компьютерные сети, смартфоны и другие устройства. Наиболее частый мотив — получение финансовой прибыли. Для этого злоумышленники используют не только информационные технологии, но и методы социальной инженерии, когда человек добровольно передает конфиденциальные данные или переводит свои сбережения. Кроме того, целью кибератак может быть выведение компьютеров или сетей из строя — из личных, коммерческих или политических побуждений.

Потерпевшими от киберпреступлений являются граждане абсолютно всех категорий, включая как социально-незащищенные слои населения (инвалиды, пенсионеры, несовершеннолетние), так и люди, занимающие руководящие посты в организациях (предприятиях) всех форм собственности.

Злоумышленниками используются изощренные способы «выманивая» денежных средств, для чего используются различные «легенды», посредством изложения которых оказывается психологическое воздействие на граждан, которые под его воздействием выполняют все команды злоумышленников. Многие из потерпевших в дальнейшем в ходе общения с сотрудниками правоохранительных органов сообщают, что действовали «под гипнозом», в результате профессиональной манипуляции со стороны преступников.

В ходе совершения преступлений злоумышленники используют звонки с номеров, визуально приближенных к номерам телефонов правоохранительных органов, служб банков (например звонки в мессенджерах с номера + 900, тогда как официальный номер Сбера 900 и т.д.), представляются официальными лицами.

Наиболее распространенными способами преступлений на сегодняшний день являются:

1. СМС от работодателя.

Потерпевшему поступает смс сообщение или сообщение в мессенджере от работодателя о том, что с ним в ближайшее время свяжется сотрудник ФСБ или иной организации, следует с ним пообщаться.

После этого потерпевшему звонит сотрудник с именем указанным руководителем и сообщает о попытках перевода личных сбережений на иностранные счета, финансирование терроризма и т.п.

В целях пресечения преступных операций потерпевшего убеждают прервать транзакции путем перевода денег (личных накоплений или путем взятия кредита) на счет, указанный злоумышленниками.

2. Злоумышленники продают Вашу квартиру или машину.

Звонившие представляются представителями службы безопасности коммерческого банка, Гос. услуг, Центрального банка либо правоохранительного органа.

Сообщают о том, что персональные данные с личного кабинета утекли и теперь преступники могут от Вашего имени продать квартиру, машину, используя электронноцифровую подпись.

В целях защиты имущества следует срочно его продать, перевести деньги на «защищенный канал», «безопасный счет», «резервную ячейку».

3. Перевод денег на «безопасный счет».

Звонившие представляются либо представителями службы безопасности коммерческого банка, Центрального банка либо правоохранительного органа и сообщают, что мошенники с использованием персональных данных потерпевшего оформляют кредиты в различных банках и для того, чтобы предотвратить хищение денег с банковского счета необходимо личные сбережения срочно перевести на «безопасные счета». В ходе дальнейшего общения потерпевшему сообщают о необходимости оформления кредитов и их перевода. Также зарегистрированы случаи продажи недвижимости и перевода мошенникам вырученных средств.

Следует отметить, что общение потерпевшего со злоумышленниками является длительным, в некоторых случаях осуществляется в течение нескольких месяцев, используется как телефонная связь, так и общение посредством мессенджеров (Ватсап, Вайбер, Телеграм и т.д.),

Кроме того, следует помнить, что «безопасных счетов» не существует, а представители Центрального Банка не осуществляют работу с физическими лицами.

4. Звонок злоумышленника под видом мобильных операторов, которые сообщают, что срок действия вашей сим-карты истек либо истекает, а для его продления необходимо сообщить код, который поступит в смс либо пройти по ссылке, иначе сим-карта будет заблокирована,

Важно знать, что у сим-карты нет срока действия, сотовые операторы перевыпускают сим-карты только по просьбе потребителей в случае физического износа, потери, необходимости другого формата.

Выполнив требования мошенников и сообщив код из смс, либо пройдя по ссылке Вы отдаете в руки злоумышленников доступ в свой личный кабинет на сайте оператора связи, после чего мошенники имеют возможность устанавливать переадресацию сообщений на нужный им номер, что позволит сменить пароль от мобильного банка и похитить денежные средства.

Вторая разновидность таких преступлений - получение в результате сообщения кода из смс доступа к аккаунту «госуслуг», дальнейшее оформление заявок на кредиты в банках, получение к персональным данным, таким как сведения о доходах, наличие банковских счетов и т.д.

5. Взлом либо копирование аккаунта пользователя в мессенджерах ватсап, вайбер, телеграмм, социальных сетей вконтакте и дальнейшее направление сгенерированных искусственным интеллектом (нейросетью) голосовых сообщений от имени потерпевшего, которое полностью копирует его голос, используя при этом ранее отправленные сообщения владельца аккаунта. Далее по типичной схеме — просьба одолжить взаймы, фото банковской карты для перевода денежных средств.

В данной ситуации важно убедиться, что общение происходит со знакомым путем звонка по мобильной сети. Сделав это, Вы обезопасите себя и предупредите знакомого о том, что от его имени действуют мошенники.

Для того, чтобы не потерять контроль над Вашим аккаунтом никогда не переходите по незнакомым ссылкам, не скачивайте программы из неподтвержденных источников, используйте двухфакторную аутентификацию Ваших аккаунтов.

Будьте максимально внимательны, поскольку следующим этапом использования искусственного интеллекта может явиться генерация видеоизображений и рассылка видео сообщений от имени родных, коллег, знакомых и т.д.

6. Хищение денежных средств через систему быстрых платежей (СБП).

Например, покупатель на сайте оставляет заявку на приобретение товара, ему поступает звонок якобы от сотрудника магазина, предлагается скидка на товар, но только при условии оплаты через СБП или QR-код. Далее злоумышленник присылает в мессенджер ссылку, ведущую на страницу с формой оплаты по QR-коду. Покупатель подтверждает платеж и денежные средства поступают на счет мошенника.

Важно в такой ситуации связаться со службой поддержки онлайн-магазина, через официальный сайт или приложение. Не сохранять для оплаты в личных кабинетах банковские карты, при возможности заведите отдельную карту для оплаты покупок онлайн.

7. Заработок на бирже, заманивание прибыльными инвестициями.

Преступниками в сети Интернет создается максимальная видимость, что общение происходит с представителями крупных инвестиционных площадок, их сайты имеют видимое сходство с банковскими организациями (например, Газпроминвестиции, РБК-инвестиции, Т-Банкинвестиции и т.д.), назначается личный брокер, общение с которым может осуществляться даже посредством видеозвонков. Под их руководством создается личный кабинет на торговой площадке, в котором отображаются все внесенные денежные средства, и прибыль. Однако их дальнейший вывод невозможен.

8. Схема «Ваш родственник попал в ДТП».

Наиболее подвержены данному виду преступлений пожилые граждане. Злоумышленник представляется либо родственником потерпевшего, либо представителем правоохранительного органа. В ходе разговора с потерпевшим сообщает, что для освобождения от уголовной ответственности и наказания в виде лишения свободы срочно необходимо передать денежные средства. Далее потерпевший, будучи введенным в заблуждении и находясь в стрессовой ситуации, действует по указаниям мошенника, денежные средства переводит либо на указанные счета, либо передает «курьерам».

Стоит еще раз обратить внимание, что жертвой кибермошенников может стать каждый, вне зависимости от возраста, образования, социального положения и прочих факторов. Причина в том, что мошенники воздействуют на эмоции человека, а современные технологии позволяют сделать используемые приемы максимально правдоподобными.

Однако противостоять им можно, для этого следует придерживаться ряда простых правил:

1. Никому и никогда не сообщайте свои паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или смс-код. Сотрудники банков и госструктур никогда не запрашивают такую информацию.

2. Не публикуйте конфиденциальные данные в соцсетях и на каких-либо сайтах.

3. Не храните данные карт и пин-коды на компьютере или в смартфоне.

4. Если с неизвестного номера звонит сотрудник банка, правоохранительных органов или государственной организации с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от Вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет и т.д.) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку.

5. Если подозреваете, что вам звонит мошенник, перезвоните в банк или в контакт-центр ведомства, сотрудником которого представлялся звонящий.

6. Не используйте слишком простые пароли, а также одинаковые пароли для разных учетных записей.

7. Защищайте свои аккаунты с помощью двухэтапной аутентификации в технических сервисах, где это возможно. В таком случае мошенники не смогут получить к ним доступ, даже если узнают пароль.

8. Совершайте покупки в интернет-магазинах только на проверенных сайтах. Сравнивайте адреса сайтов, так как в адресах может отличаться одна буква или точка.

9. Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, проголосовать или получить какую-либо выплату.

Если же средства уже переведены мошенникам:

1. Немедленно заблокируйте карту с помощью мобильного приложения, личного кабинета на сайте банка или через контакт-центр банка по телефону.

2. В течение суток после получения сообщения о списании средств напишите заявление в отделении банка о несогласии с операцией и возврате денежных средств. Также обратитесь с заявлением о хищении денег в любое отделение полиции.

Современный мир и технологии не только дарят нам бесконечный доступ к информации, но и ждут от нас умения ими пользоваться. Развитие критического мышления, соблюдение простых правил информационной гигиены, бдительность и забота об окружающих помогут избежать проблем и не стать жертвой кибермошенников.

Методические рекомендации подготовлены управлением по надзору за уголовно-процессуальной и оперативно-разыскной деятельностью прокуратуры области.