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, имеющие несколько высших образований.

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 на Вайбер с номера +900, 9ОО, тогда как официальный номер Сбербанка 900 и т.д.), представляются официальными лицами.

-хищение денег и имущества под предлогом обновления банкнот (звонок от мошенников с указанием о необходимости проверки подлинности банкнот Банка России, для чего убеждают установить стороннее приложение, посредством которого получают удаленный доступ к телефону жертвы; также используется поквартирный обход от якобы специалистов социальных служб, которые убеждают обменять денежные купюры на поддельные);

- использование ложных аккаунтов руководителей Банка России, правоохранительных органов, органов прокуратуры, содержащих реальные данные, взятые из открытых источников (фамилию, имя, отчество, фото);

- сообщение клиентам банков об утечке персональных данных;

- обещание помочь с компенсацией ранее похищенных денег;

- обмен кэшбека на рубли.

БУДЬТЕ БДИТЕЛЬНЫ!!!!!

@KRPRO_PRAVZN

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 звонит сотрудник с именем указанным руководителем и сообщает о попытках перевода личных сбережений на иностранные счета / финансирование территоризма / украины и тп.

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 электронно-цифровую подпись.

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

3. Перевод денег на «безопасный счет», якобы для их сохранности.

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.).

Еще одна разновидность преступной схемы – когда **звонят якобы сотрудники правоохранительных органов и сообщают что в отношении Вас возбуждено уголовное дело в связи с финансированием экстремисткой, террористической деятельности,** поскольку с Вашего банковского счета осуществлен перевод денежных средств в недружественное государство.

В ходе общения злоумышленники могут присылать якобы фото удостоверений, повесток, постановлений о возбуждении уголовного дела, подписок о неразглашении следственной тайны и т.д. Нужно быть предельно внимательными, не поддаваться манипуляциям и проверять сообщаемую информацию,

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, в противном случае 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. Сдача налоговых деклараций и справок о доходах.

Звонившие представляются сотрудниками Госуслуг, управления по делам президента, сообщают, что в рамках декларационной компании проверяют персональные данные лиц, сдавших налоговые декларации либо декларации о доходах.

Со слов преступников - для подтверждения следует назвать паспортные данные и код из СМС.

Результат – списание денег со счетов, взятие кредита.

6. **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.

А дальше все по типичной схеме – просьба одолжить взаймы, фото банковской карты для перевода денежных средств.

В данной ситуации важно убедиться, что вы общаетесь именно с Вашим 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 видеосообщений от имени родных, коллег, знакомых и т.д.

7. **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-коду, затем 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.

8. Широко получившая последнее время схема, в результате использования которой причиняется наиболее крупный ущерб – **заработок на бирже, заманивание прибыльными инвестициями**. Преступниками создается максимальная видимость того, что общение происходит с представителями крупной инвестиционной площадки, их сайты имеют видимое сходство с банковскими организациями (например, Газпроминвестиции, РБК-инвестиции, Тинькофф-инвестиции и т.д.), назначается личный брокер, общение с которым может осуществляться даже посредством видеозвонков. Под их руководством создается якобы личный кабинет на торговой площадке, в котором отображаются все внесенные денежные средства, и прибыль. Однако их дальнейший вывод невозможен.

Например, жительница г. Сосновоборск в сети интернет увидела псевдорекламу «Газпромбанка» о дополнительном заработке, ввела свои паспортные данные на сайте. спустя несколько дней с ней связался сотрудник торговой компании и рассказал о возможном росте финансовых накоплений в ходе торгов и дальнейшего вывода прибыли. Заинтересовавшись, женщина установила инвестиционную платформу и стала сотрудничать якобы с финансовым специалистом через приложение «скайп». Первоначально внесла депозит в размере 10 тыс, после чего увидела прибыль в размере 2 тыс, которые ей поступили на банковскую карту. Это придало веру в возможность зарабатывать. Обманутая женщина вносила личные денежные средства, которые получила путем оформления кредитов в различных банках, думая, что торгует газом, нефтью, серебром, акциями «Газпрома». В дальнейшем, при оформлении сделок, система стала выдавать ошибки. Лже-специалисты поясняли, что необходимо оформить страховку и ряд других финансовых манипуляций, однако работа на платформе была заблокирована. Действуя по инструкции мошенников, потерпевшая перевела более 6 млн. руб.

9. Рассылка налоговых писем о выявлении подозрительных транзакций и активности налогоплательщика.

В поддельном сообщении предлагается пройти дополнительную проверку и предоставить сведения по запросу налоговой службы. Так мошенники могут запросить кассовые документы, счета-фактуры, отчетные документы.

Далее для прохождения проверки предлагается обратиться к указанному в письме инспектору под угрозой блокировки счетов налогоплательщика.

Важно помнить, что ФНС не рассылает такого рода письма и не имеет отношения к ним, такие письма открывать не рекомендуется, как и переходить по ссылкам.

8. Схема «**Ваш родственник попал в ДТП**», наиболее подвержены данному виду преступлений пожилые граждане. Злоумышленник представляется либо родственником потерпевшего либо представителем правоохранительного органа и сообщает, что для освобождения от уголовной ответственности и наказания в виде лишения свободы срочно необходимо передать денежные средства.

ВАЖНО ЗНАТЬ!!!!

Используемые мошенниками схемы постоянно меняются, «подстраиваясь» под общественно-политическую обстановку, значимые события в государстве.

Прокуратура Тужинского района Кировской области поддержала государственное обвинение по уголовному делу в отношении 32-летнего местного жителя.

Он осужден по ч. 3 ст. 30, ч. 2 ст. 167 УК РФ (покушение на умышленное уничтожение чужого имущества путем поджога, повлекшее причинение значительного ущерба).

Установлено, что подсудимый, в один из дней февраля 2023 года, будучи в состоянии алкогольного опьянения, имея личные неприязненные отношения к своей бывшей супруге, решил причинить последней имущественный вред.

В ходе своего преступного умысла, подсудимый проник в тамбур одной из квартир деревянного дома, где проживала его бывшая супруга, совершил поджег и скрылся с места преступления. Однако, довести до конца свой преступный умысел не смог в связи с локализацией возгорания пожарными.

В процессе пожара было повреждено и уничтожено имущество собственников жилых помещений многоквартирного дома.

Суд согласился с мнением государственного обвинителя прокуратуры Тужинского района и назначил наказание в виде лишения свободы сроком на 1 год 6 месяцев.

С учетом данных о личности, наличия на иждивении малолетнего ребенка и иных данных, суд посчитал возможным применить положения ст. 73 УК РФ (условное осуждение), установив испытательный срок 2 года.

Также, судом удовлетворены гражданские иски потерпевших о возмещении имущественного и морального вреда, причиненного преступлением, на сумму более 130 тысяч рублей.

Приговор суда не вступил в законную силу.

После вмешательства прокуратуры восстановлено освещение улиц пгт Тужа

Поводом к проведению проверочных мероприятий и принятия мер реагирования послужило поручение заместителя прокурора Кировской области Сергея Ломовцева по итогам состоявшегося личного приема местных жителей.

В ходе проверки сведения о ненадлежащем освещении ряда улиц пгт Тужа в вечернее и ночное время подтвердились.

В целях устранения выявленных нарушений прокурором Тужинского района главе администрации городского поселения внесено представление, по результатам рассмотрения которого выявленные нарушения устранены, освещение на улицах поселка восстановлено.

Прокурором Тужинского района утверждено обвинительное заключение по резонансному делу в отношении местной жительницы.

Поводом для возбуждения уголовного дела явилось поступившее в органы следствия сообщение о совершении преступлений, предусмотренных п. «б» ч. 4 ст. 132 УК РФ (насильственные действия сексуального характера, совершенные в отношении лица, не достигшего 14-тилетнего возраста),

п.п. «а», «г» ч. 2 ст. 242.1 УК РФ (изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних).

Согласно материалов дела, обвиняемая 32-летняя жительница пгт. Тужа Кировской области совершила указанные деяния в отношении своей малолетней дочери.

В сентябре 2023 года обвиняемая задержана и ей избрана мера пресечения в виде заключения под стражу.

15.04.2024 года прокурором района по данному уголовному делу утверждено обвинительное заключение, 17.04.2024 уголовное дело направлено в суд для рассмотрения по существу в общем порядке судебного разбирательства.

Яранским районным судом вынесен приговор в отношении арендатора лесного участка, совершившего незаконную рубку лесных насаждений в особо крупном размере.

Яранским районный судом вынесен обвинительный приговор в отношении арендатора лесных участков Михайловского участкового лесничества Яранского лесничества, который признан виновным в совершении преступления, предусмотренных ч. 3 ст. 260 УК РФ.

В ходе расследования уголовного дела установлено, что подсудимый, являясь индивидуальным предпринимателем, осуществляющим деятельность в сфере заготовки и сбыта древесины, в период с 16.02.2017 по 31.03.2017 на территории Михайловского участкового лесничества Яранского лесничества министерства лесного хозяйства Кировской области на арендуемом лесном участке организовал незаконную выборочную рубку хвойных лесных насаждений, что повлекло причинение ущерба министерству лесного хозяйства Кировской области в особо крупном размере на общую сумму 577 115 рублей.

Несмотря на непризнание вины подсудимым, с учетом совокупности представленных стороной обвинения доказательств, суд согласился с мнением государственного обвинителя о доказанности вины подсудимого в совершении преступления, признал его виновным и назначил наказание в виде штрафа в размере 1 000 000 рублей.

По ходатайству государственного обвинителя суд применил положения ст. 104.1 УК РФ (конфискация имущества), обратив в собственность государства на основании обвинительного приговора 4 бензопилы, 3 единицы лесозаготовительной техники.

Судом удовлетворено исковое заявление министерства лесного хозяйства Кировской области о взыскании ущерба, причинённого незаконной рубкой в размере 577 115 рублей.

Не согласившись с приговором, подсудимым подана апелляционная жалоба, которая 20.02.2024 судебной коллегией по уголовным делам Кировского областного суда отклонена, приговор оставлен без изменения, он вступил в законную силу.

Прокуратура Тужинского района поддержала обвинение по уголовному делу в отношении ранее дважды судимого за преступления против личности (ст. 116.1, 117, 119 УК РФ) 46-летнего местного жителя.

Он вновь признан виновным по ч. 2 ст. 116.1 УК РФ (совершение иных насильственных действий, причинивших физическую боль, лицом, имеющим судимость за преступление, совершенное с применением насилия).

В суде установлено, что подсудимый, находясь 4 декабря 2023 в состоянии алкогольного опьянения в квартире своей матери в одном из жилых домов по ул. Мира с. Шешурга Тужинского района, спровоцировал конфликт, после чего нанес удар рукой в голову пожилой женщины, причинив ей физическую боль.

Ранее он привлекался к уголовной ответственности за аналогичные преступления, отбывал наказание в виде лишения свободы в исправительной колонии, откуда освободился за несколько дней до совершения инкриминируемого преступления (25.11.2023)

Вину в содеянном мужчина полностью признал.

Суд согласился с мнением государственного обвинителя прокуратуры и, с учетом совокупности смягчающих наказание обстоятельств, назначил наказание в виде 7 месяцев ограничения свободы с возложением административных ограничений в виде запрета на выезд за пределы муниципального образования (по месту жительства или пребывания).

Прокуратура Тужинского района поддержала гособвинение по уголовному делу в отношении 37-летнего местного жителя. Он признан виновным по ч. 1 ст. 327 УК РФ (использование заведомо подложного документа).

В суде установлено, что 23 января 2024 года подсудимый управлял автомобилем МАЗ и был остановлен сотрудниками полиции.

В момент проверки документов он, желая скрыть обстоятельства административных правонарушений, предусмотренных ст.ст. 12.3 и 12.31.1 КоАП РФ, предоставил инспекторам собственноручно написанный путевой лист, осознавая недостоверность имеющихся в нем записей о якобы пройденном предрейсовом медицинском осмотре и техническом осмотре эксплуатируемого транспортного средства.

Суд согласился с мнением государственного обвинителя прокуратуры и признал подсудимого виновным.

Принимая во внимание тяжесть содеянного, данные о личности, совокупность смягчающих наказание обстоятельств, суд назначил наказание в виде штрафа в размере 10 тыс. рублей.